Deutsche
Stiftung
Friedensforschung
DSF
german foundation for peace research

Sicherheit durch Verschleierung.
Warum Regierungen Proxies in Cyberkonflikten einsetzen

Sebastian Harnisch und Kerstin Zettl-Schabath

Forschung DSF № 57

Kontakt:
Deutsche Stiftung Friedensforschung (DSF)
Am Ledenhof 3-5
49074 Osnabrück
+49 541 60035-42
www.bundesstiftung-friedensforschung.de
info@bundesstiftung-friedensforschung.de

Prof. Dr. Sebastian Harnisch
Institut für Politische Wissenschaft
Ruprecht-Karls-Universität Heidelberg
Bergheimer Straße 58
69115 Heidelberg

Spendenkonto der Deutschen Stiftung Friedensforschung:
Bank für Kirche und Caritas eG, IBAN DE80 4726 0307 0012 0246 00

ISSN 2193-794X

Inhalt

Forschung-DSF erscheint unregelmäßig.

Zusammenfassung

Für die vorliegende Projektstudie wurde ein Datensatz (HD.CY-CON) entwickelt, der bekanntgewordene bösartige Cyberoperationen im Zeitraum zwischen 2000-2019 erfasst. Er beinhaltet 1.265 Operationen, die anhand von 43 Kategorien kodiert wurden, die Auskunft geben über Angriffsziele, angreifende und angegriffene staatliche und nichtstaatliche AkteurInnen, den Modus sowie die technische und politische Attribution (Zuschreibung) des Angriffs. Der Datensatz dokumentiert erstmals detailliert die Beteiligung von sog. Cyberproxies, Stellvertreterorganisationen, und identifiziert zeitliche Lücken in der technischen und politischen Zuschreibung von Cyberoperationen.

HD.CY-CON ergänzt bereits bestehende Datensätze vor allem in vier Bereichen: der systematischen Messung von Cyberkonfliktintensitäten, der Interaktion zwischen On- und Offlinekonfliktdynamiken sowie der Erfassung von Cyberproxyverhalten und Attributionsprozessen. In der vorliegenden Pilotstudie gehen wir anhand eines liberalen Erklärungsmodells auf die Nutzung von bestimmten Cyberproxytypen durch demokratische und autokratische Regime ein. Während letztere Cyberproxygruppen primär zur Verschleierung von Angriffshandlungen gegenüber demokratischen Regimen nutzen, setzen erstere IT-Sicherheitsfirmen als StellvertreterInnen ein um technische Attributionen vorzunehmen, ohne dass aus diesen unmittelbarer politischer Handlungsdruck entsteht.

Die Pilotstudie plausibilisiert das liberale Erklärungsmodell anhand von zwei vergleichenden Studien zum Proxyeinsatz durch die russische und chinesische Regierung sowie amerikanische und israelische Administrationen im Zeitverlauf, die bemerkenswerte Gemeinsamkeiten und Unterschiede zwischen aber auch innerhalb der Regimetypen zeigen. Dem liberalen Modell liegt die Annahme zugrunde, dass autokratische und demokratische Regime aufgrund ihrer unterschiedlichen Legitimationserfordernissen (starke) Anreize haben, ihr Cyberkonfliktverhalten zu verschleiern oder zu verheimlichen, sodass auch weiterhin ein erheblicher Teil bösartiger Operationen unentdeckt, undokumentiert und/oder unveröffentlicht bleiben dürfte. Generalisierende Erkenntnisse, die aus diesem oder anderen Datensätzen gewonnen wurden, sollten daher mit großer Vorsicht interpretiert werden, weil sie ggfs. nur jenes Konfliktgeschehen abbilden, welches die Konfliktbeteiligten mit einer breiteren Öffentlichkeit teilen wollten.

Der Datensatz HD.CY-CON wurde in englischer Sprache angelegt und wird mit einem englischsprachigen Codebuch, welches den Kodierprozess näher beschreibt, dauerhaft auf dem Forschungsdatenportal der Universität Heidelberg zur Verfügung gestellt (https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB). Der Datensatz wird im Zuge von Anschlussprojekten aktualisiert, gepflegt und erweitert werden, sodass er für die evidenzbasierte quantitative und qualitative Cyberkonfliktforschung eine wichtige Datengrundlage wird bilden können.

Abstract

The dataset HD.CY-CON covers malicious cyber operations, which came to be known, between 2000 and 2019 by state and non-state actors. It specifically documents initiating and receiving actors of cyber-crime, cyber espionage and cyber sabotage operations, the respective modus operandi, an intensity score as well as a detailed categorization of the technical and political attribution process. Overall, it consists of 1.265 incident descriptions, using 43 different categories to highlight the prominent role of different types of cyber proxies in obfuscating or concealing the attribution of cyber operations.

HD.CY-CON supplements existing datasets on cyber conflict behavior in four areas: measuring cyber conflict intensity, the interaction between On- und Offline conflict dynamics as well as cyber proxy behavior and detailing attribution processes. In this pilot study, we use a liberal explanatory model to examine the use of cyber proxies by democratic and autocratic regime types. Whereas autocratic regimes use cyber proxies to obfuscate offensive operations vis-à-vis democratic regimes, the latter utilize the advantage of IT-security providers to technically attribute operations that do not create political pressure for an escalatory response.

This pilot study is a plausibility probe for our liberal explanatory model, using two comparative case studies for autocratic regimes (the Russian Federation and the People's Republic of China) and democratic regimes (Israel and the United States) to examine commonalities and differences among and between regime types in their use of cyber proxies. The liberal model assumes that autocratic and democratic regimes, because of their different legitimatory models, do have (strong but differing) incentives to obfuscate or conceal their cyber conflict behavior. It follows that generalized findings, which are based on this or other existing data sets, should be interpreted with utmost carefulness because these data sets (may) represent only those operations which the interested parties wanted to become known.

For wider accessibility, HD.CY-CON is presented in English language and with a detailed codebook. Both may be downloaded on the research data repository of Heidelberg University (https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB). The data set will be updated, maintained and extended in the future so that it may serve for the cyber conflict research community in both quantitative and qualitative studies.

1. Zur Relevanz des Datensatzes & Zielsetzung des Projekts

Kommerzielle Threat-Intelligence von IT-Unternehmen sammelt seit geraumer Zeit vielfältige Daten über Cyberangriffe, darunter auch jene, die von den Angriffszielen nicht öffentlich gemacht wurden. Diese Analysen, die auch den Zweck verfolgen (z.B. Kaspersky`s „Targeted Cyberattacks Logbook") die Schutzdienstleistungen der Unternehmen gegen eben diese Angriffe zu bewerben, sind erst in den vergangenen zehn Jahren durch wissenschaftliche Beiträge ergänzt worden. Zum Zeitpunkt der Beantragung des hier vorgestellten Forschungs-projektes steckte die quantitativ-qualitative Cyberkonfliktforschung daher noch in den Kinder-schuhen: trotz vereinzelter Versuche, Cyberkonflikte quantitativ zu erfassen, stützte sich die Forschung in erster Linie auf anekdotische Evidenzen von Einzelfall- oder vergleichenden Small-N-Studien (z.B. Farwell und Rohozinski 2011; Lindsay 2013; Bronk und Tikk-Ringas 2013).

Erst 2014 entwickelten Brandon Valeriano und Ryan Maness einen ersten systematischen Cyberkonfliktdatensatz (Dyadic Cyber Incident and Campaign Dataset, kurz: DCID), der auf Grundlage von Open-Source-Informationen umfangreichere Daten über staatliche Cyberoperationen sammelte. Die Veränderung des Konfliktgeschehens, insbesondere die starke Beteiligung nichtstaatlicher Akteure während des Sony-Hacks (2014), der Abschaltung kritischer Infrastruktur in der Ukraine (Stromkraftwerke Ende 2015 & 2016) und der Hack gegen das Democratic National Committee im Vorfeld der US-Präsidentschaftswahlen 2016, zeigten indes, dass der staatszentrierte Ansatz von Valeriano und Maness einige wichtige AngreiferInnen¬kategorien nicht ausreichend erfasste und die Attribution von Angriffen nicht differenziert genug betrachtete. So wurden bei den genannten Cyberoperationen zwar Staaten politisch verantwortlich gemacht, aber deren Einsatz von sogenannten Cyberproxies, i.e. Stell-vertretern) verhinderte eine weitergehende oder gar effektive Reaktion auf die Angriffe. Der Einsatz von Cyberproxies, so schien es, verhinderte (einstweilen) Eskalationsdynamiken im Cyberraum, sodass eine weitere mögliche Erklärung für die vergleichsweise geringe Konflikt-intensität von Cyberkonflikten in greifbarer Nähe erschien (Rid 2013; Valeriano und Maness 2015).

Das sogenannte Attributionsproblem, das neben der cyberforensischen Hürde der Bestimmung von TäterInnen und Vorgehen auch oft die nicht erfolgte öffentliche und politische Zuweisung umfasst (Rid und Buchanan 2015; Egloff 2020), erfuhr daher in der sozialwissenschaftlichen Forschung immer mehr Aufmerksamkeit. Diese Forschung begriff Attribution nicht mehr nur als eine rein technische Handlung, sondern nahm nun die ökonomischen, politischen und psychologischen Erwägungen und Hemmnisse in Attributionsprozessen in den Blick (Rid und Buchanan 2015; Lin 2016; Berghel 2017; Edwards et al. 2017; Mueller et al. 2019; Egloff 2020; Egloff und Smeets 2021).

Vor diesem Hintergrund entwickelte das vorliegende Projekt einen Cyberkonfliktdatensatz, der zum einen systematisch nichtstaatliche AkteurInnen (als AngreiferIn und Angegriffene) einschloss und zum anderen unterschiedliche Attributionsformen (technische/politische) im Zeitverlauf indizierte. HD-CY.CON erfasst für den Zeitraum von 2000 bis 2019 bislang 1.265 Cybervorfälle mit politischer Dimension, d.h., dass ein Akteur diesen Angriff sprachlich oder durch Praxis zum Gegenstand der politischen Auseinandersetzung gemacht hat. Der Datensatz soll es ermöglichen, folgende Fragen zu beantworten: Wer attribuiert welche Cyberoperationen wann, auf welche Weise und mit welchen Konsequenzen?

Dieser granulare Fokus auf die zahlreichen Schattierungen öffentlicher Attributionsprozesse bildet den großen Mehrwert des HD-CY.CON: Im Vergleich zu anderen Datensätzen werden mehr Cyberoperationen (auch jene von nicht-

staatlichen AkteurInnen), differenzierter (jene die politisiert werden) und analytisch anspruchsvoller (jene die nur technisch attribuiert werden, werden von jenen die auch politisiert werden, hinsichtlich dieser technischen vs. politischen Attribution getrennt erfasst) aufbereitet, sodass akteurspezifische und temporale Interaktions-dynamiken sehr viel besser erkannt und untersucht werden können.

Neben der Konzeptualisierung und Pflege des Datensatzes legte das Forschungsprojekt seinen Schwerpunkt auf den (offensiven) Einsatz von Cyberproxies durch autokratische Regime und defensive Reaktionspraktiken mit Hilfe von StellvertreterInnen durch demokratische Regime. Sogenannte „Cyberproxies" erhielten erst ab 2016 gesteigerte Aufmerksamkeit durch die politikwissenschaftliche Cyberkonfliktforschung (u.a. Maurer 2016; Maurer 2018; Borghard und Lonergan 2016; Collier 2017). Desiderate der Forschung waren die theoretische Erklärung des Einsatzes unterschiedlicher Proxytypen (Maurer 2016) sowie die evidenzbasierte und quantitativ-datengestützte Analyse des Konfliktverhaltens, die über Einzelfallstudien hinaus die Identifikation von Konfliktinteraktionsmustern in unterschiedlichen Dyaden und Regionen (z. B. Enduring Rivalries), über unterschiedliche Angriffsarten (etwa Cyberkriminalität und Spionage) oder Akteurstypen (Regimetypen oder Angreifer/Angegriffene) erlaubt.

Das Projekt verfolgte daher auch das Ziel, die primär deskriptive Cyberkonfliktforschung durch ein quantitatives Vorgehen zu ergänzen und mit Hilfe eines liberalen theoretischen Ansatzes zu erweitern, der unterschiedliche Staaten-Proxy-Beziehungen auf unterschiedliche Pfade der Herrschaftssicherung von demokratischen und autokratischen Regimetypen zurückführt. Dabei gehen wir von der Annahme aus, dass beide Regimetypen jeweils bestimmte Proxytypen einsetzen, um durch Geheimhaltung unterschiedliche Informationsasymmetrien auszugleichen: Autokratien setzen Proxies offensiv ein, um ihre Täterschaft gegenüber der internationalen Gemeinschaft und dem Angriffsziel zu verheimlichen; demokratische Regime nutzen Proxies (primär) defensiv, um ihre Viktimisierung gegenüber der eigenen Gesellschaft zu verschleiern (siehe unten Abschnitt 5.3).[1]

Der nun für die Forschungsgemeinde zugängliche Datensatz HD-CY.CON bietet also nicht nur die Möglichkeit, systematisch das Konfliktverhalten unterschiedlicher Regimetypen zu vergleichen, sondern mit Blick auf unterschiedliche Attributionspraktiken auch zeitliche Varianzen aufzudecken. Wir begannen die Analyse der Instrumentalisierung offensiv agierender Cyberproxies durch Autokratien mit einer Untersuchung von Hacking-Operationen durch China und Russland (most likely cases). Für den defensiven Einsatz von Cyberproxies durch demokratische Regierungen lag der Fokus auf der (stellvertretenden) technischen privater IT-Unternehmen. Während die rezente Forschung zumindest empirisch schon den offensiven Gebrauch von Cyberproxies durch autokratische Regime festgestellt hatte (bspw. Maurer 2016), fehlte ein Modell zur theoretischen Erklärung als auch zur systematischen Erfassung des (defensiven) Gebrauchs von Proxies durch demokratische Regierungen. Im Folgenden setzen wir uns daher zunächst konzeptionell genauer mit dem sogenannten „Attributionsproblem" im Cyberraum auseinander, um zu verdeutlichen, welche Anreize für demokratische Regierungen bestanden, die technische Attribution von Angriffen regelmäßig privaten IT-Unternehmen zu überlassen.

[1] Wir verstehen Geheimhaltung dabei als „bewusste Verheimlichung von Informationen gegenüber einem oder mehreren Publika" (Carson 2020: 5), die auf einem Spektrum zwischen ausbleibender Offenlegung und bewusster Geheimhaltungs¬infrastruktur, z. B. Verschlüsselung, unterschiedliche Formen annehmen kann: „offenen Geheimnissen", i.e. bekannten Fakten ohne öffentliche Bestätigung, „Quasi-Geheim-nissen", i.e. öffentliche Geheimhaltung verbunden mit Teiloffenlegungen (leaks), „Verschleierungen", i.e. Informationsverzerrung, und „Täuschung", d.h. der bewussten Informationsveränderung (Carnegie 2021: 215).

2. Verantwortungszuweisung im Rahmen von Cyberkonflikten: Attribution

Im Cyberspace, der sogenannten „Fifth Domain", gelten in Teilen andere Regeln als in den „natürlichen" Konfliktdomänen (Healey 2012). Im Falle eines konventionellen Militärschlages ist es den angegriffenen Konfliktparteien zumeist möglich, den Ursprung und damit auch den Urheber der Attacke rasch und zweifelsfrei zu identifizieren. Dies gilt nicht nur für Konfliktinteraktionen in bereits andauernden, gewaltsamen Konflikten, in welchen der jeweilige „Feind" bereits klar identifiziert und als solcher kommuniziert worden ist, sondern auch für die meisten Fälle konventioneller Erstschläge, wie das Abfeuern einer Rakete. Im Cyberraum sind diese „technischen Zuweisungen" durch zahlreiche Besonderheiten erschwert. Regelmäßig werden in Cyberoperationen keine materiellen Waffen mit Seriennummern oder klar identifizierbaren Produktstandards (Kalibern) eingesetzt. Auch müssen keine Militärangehörigen mit eindeutig nachweisbarer Affiliation über Insignien beteiligt sein. Im Vergleich zu Offline-Operationen zielen Online-Angriffe zumeist darauf, längere Zeit unerkannt zu bleiben, sofern sie nicht disruptive Wirkung entfalten sollen. Schon die technische Attribution setzt also Detektion voraus. Ohne eine erkennbare Tat, wird die Frage nach möglichen TäterInnen gar nicht erst gestellt (Rid und Buchanan 2015; Goel und Nussbaum 2021).

Der Cyberraum als Konfliktdomäne weist einige Besonderheiten auf, welche die Attribution von böswilligen Operationen deutlich erschweren: Als einzige von Menschen selbst erschaffene Konfliktdomäne unterliegt diese nicht nur einer ständigen Veränderung, Erweiterung und Vertiefung, sondern die Struktur des Konfliktraumes Cyberspace als Netzwerk von Netzwerken ist auf Anonymität und Dezentralität angelegt, sodass Angriffe schwer zu erkennen (Detektion), einem bestimmten Akteur technisch zuzuweisen (technische Attribution) und politische und rechtliche Verantwortung zuzurechnen sind (politische u. rechtliche Attribution), bevor diese abgeschreckt oder (legitime) Gegenmaßnahmen ergriffen werden können. Technologischer Fortschritt und die Digitalisierung immer weiterer Lebensbereiche erweitern daher stetig das Tableau potenzieller Angriffsziele und Angriffsarten, sog. Angriffsvektoren, so dass CyberangreiferInnen unentdeckt bleiben können (Baram und Sommer 2019). Auch wenn es in der Cyberforensik in den letzten Jahren zu einer erheblichen Ausweitung privatwirtschaftlicher und staatlicher Attributionskapazitäten gekommen ist (z.B. im Rahmen der „internal detection", Buchanan 2017), und sich Cyberoperationen immer genauer einer bestimmten IP-Adresse in einem bestimmten Land zuordnen lassen, bleiben weiterhin erhebliche Hürden auf dem Weg zur sogenannten „True Detection" bestehen (Lee 2016), i.e. einer konkreten politischen Verantwortungszuweisung an einen bestimmten nichtstaatlichen und/oder staatlichen Akteur. Konkretes Beispiel für diese Unwägbarkeiten sind sogenannte „False-Flag"-Attacken, im Rahmen derer CyberakteurInnen Angriffstaktiken nutzen, die gemeinhin anderen AngreiferInnen zugesprochen werden, um die Opfer auf eine falsche Attributionsfährte zu locken (Bartholomew und Guerrero-Saade 2016).

Fortschritte in der Cyberforensik in den letzten Jahren haben privatwirtschaftliche IT-Sicherheitsunternehmen dazu bewegt, trotz weiterhin bestehender Restzweifel, zunehmend technische Verantwortungszuweisungen mit Konfidenzintervallen zu versehen und darüber-hinaus auch Aussagen darüber zu treffen, welche AkteurInnen potentiell den größten Nutzen aus der jeweiligen Operation ziehen könnten (Steffens 2018, S. 81).

Wachsen die technischen Fähigkeiten der Cyberforensik, bleiben technische und/oder politische Attributionen staatlicher Organe, insbesondere in demokratischen Zielstaaten, aber

aus, oder variieren diese zumindest über Zeit, so stellt sich die Frage, wie die temporalen und funktionalen Lücken zwischen technischer und politischer bzw. rechtlicher Zuschreibung sowie den angeschlossenen (verteidigungs-)politischen Reaktionen zu erklären sind.

Die Annahme unseres Projektes war es hier, dass Attributionsakte sensitive Informationen preisgeben, die das Verhalten von anderen Staaten und nichtstaatlichen AkteurInnen zum Nachteil des Attribuierenden verändern können (Carnegie und Carson 2020, S. 2). Entscheidend für die Attribution (und die Nutzung bestimmter Proxytypen) ist nun, dass die Kostenverteilung für die Preisgabe sensitiver Informationen zwischen autokratischen und demokratischen Regimen variiert: Für Autokratien sind die Kosten einer Preisgabe von sensitiven Informationen über Cyberaktivitäten innerstaatlich grundsätzlich gering(er), denn sie unterliegen nicht den Transparenzgeboten demokratischer Rechtstaatlichkeit und auch die Offenlegung von Cyberüberwachungsfähigkeiten, die gegen die eigene Bevölkerung eingesetzt werden könnte, ist ebensowenig kostenträchtig, weil entsprechende Opposition leichter unterbunden werden kann. Für autokratische Regime sind sensitive Informationen lediglich dann kostenträchtig, wenn sie Cyberangriffe auf internationale (und zumeist demokratische) Ziele aufdecken, die sie zur Rechenschaft ziehen könnten. Um diese Kosten zu vermeiden, setzen Autokratien offensive Cyberproxies ein, um ihre Verwicklung zu verschleiern, d.h. konkret Informationen über den staatlichen Angriffsauftrag zu verheimlichen, um so einer politischen und rechtlichen Verantwortungszuweisung zu entgehen.

Demokratien sind kostensensibler für die Offenlegung von Cyberaktivitäten, nicht zuletzt seit dem Bekanntwerden weitreichender Überwachungsprogamme der National Security Agency (NSA) im Jahr 2013. Attribuieren demokratische Staaten fremde Cyberangriffe, so müssen sie fürchten, dass die zugrundeliegenden technischen Fähigkeiten Gegenstand der öffentlichen Debatte werden, insbesondere insofern diese Informationen nahelegen, dass die Fähigkeiten auch gegen eigene Bürger oder andere (befreundete) Demokratien eingesetzt worden sind oder werden könnten. Eine solche weitergehende Offenlegung der Fähigkeiten, etwa im Rahmen parlamentarischer Untersuchungsausschüsse, ermöglicht es zudem potentiellen Angreifer¬Innen, ihre Angriffsstrategien auf die Umgehung dieser Fähigkeiten abzustimmen. Zudem birgt die Offenlegung sensitiver Informationen über Cyberangriffe für demokratische Regierungen ein höheres Risiko, dass die Information über Angriffe öffentliche Forderungen auf eine Erwiderung der Angriffe nachsichziehen, sodass eine Eskalationskontrolle erschwert wird (Harnisch/Zettl/Hansel 2022: 13-14). In der rezenten Cybersicherheitsforschung wurde die Bedeutung privater IT-Sicherheitsfirmen im Attributionsprozess zwar bereits vielfach untersucht (Lindsay 2015; Lohmann 2018; Poznansky und Perkoski 2018; Schulzke 2018; Romanosky und Boudreaux 2019). Eine systematische und theoretische Erklärung des Einsatzes als Proxies zur Veränderung der Kosten von sensitiven Informationen durch demokratische Regierungen erfolgte aber bislang nicht.

3. Bisherige Datensätze zu Cyberoperationen

Private IT-Sicherheitsfirmen stellen eine Vielzahl, statistisch oftmals jedoch nur schwer verwertbarer Cyberoperationsdaten zusammen. Diese erscheinen entweder in unregelmäßigen Einzelinzidenzmitteilungen oder hochaggregierten jährlichen Berichten, welche eine detaillierte Untersuchung von Konfliktdyaden in Fallstudien und die Identifikation von längerfristigen Entwicklungstrends erschweren. Aus diesem Grund gehen wir hier nur auf drei Cyberkonfliktdatensätze ein, die als primäre Referenz-/Orientierungs- und Abgrenzungsobjekte für die Konzeptualisierung des neuen Datensatz HD-CY.CON dienten.

Der Datensatz DCID von Valeriano und Maness wurde in seiner ersten Version für die Jahre 2000 bis 2014 so konzipiert, dass er ausschließlich nur staatliche Cyberoperationen erfasste.[2] Im Gegensatz zum DCID verspricht der Cyber Operations Tracker des Council on Foreign Relations für einen Zeitraum ab 2005 auch staatlich-gesponserte Cyberoperationen zu dokumentieren, sodass eine parallele Nutzung beider Datensätze eine umfassende Analyse (ab 2005) hätte ermöglichen sollen. Betrachtet man die Kodierungen der beiden Datensätze indes genauer, so zeigt sich, dass diese nicht hinreichend zwischen staatlichen und lediglich staatlich-gesponserten Cyberoperationen unterscheiden und in etlichen Fällen eine staatliche Involvierung aus den genannten Quellen überhaupt nicht hervorgeht.[3] Diese konzeptionelle Schwachstelle war somit u.a. Anlass für den HD-CY.CON, ein ausdifferenzierteres Spektrum an möglichen AngreiferInnen-Kategorien auszuweisen und sehr viel spezifischer zu dokumentieren, wie, wann und durch welche AkteurInnen es zu welcher Form von Attribution gekommen ist.

Ein weiterer analytischer Mehrwert des HD-CY.CON sind dessen Inklusionskriterien: So werden neben politischen, politisch-motivierten Operationen, oder Angriffen auf politische AkteurInnen selbst auch solche Fälle erfasst, die weder auf der AngreiferInnen-, noch der Opferseite politisch konnotiert sind, im weiteren Verlauf jedoch durch AkteurInnen politisiert wurden.

[2] Operationen von nichtstaatlichen AkteurInnen sollen in einer aktualisierten Version, die zum Zeitpunkt der Erstellung dieses Berichts noch nicht vorlag, berücksichtigt werden.
[3] Vgl. bspw. die Operationen „Earthquake Hack" im DCID und APT „Hellsing" im CFR Tracker.

4. Aufbau des Datensatzes HD-CY.CON

Der HD-CY.CON besteht aus Einzelinzidenzbeschreibungen von bösartigen Cyberoperationen anhand von 43 verschiedenen Kategorien, wobei die meisten davon nochmals in Subkategorien unterteilt werden (vgl. Codebuch). Somit kommen einigen dieser Kategorien mehrere Spalten zu, da oftmals nicht nur eine Receiver-Kategorie, i.e. ein Angriffsziel, von einer Cyberoperation betroffen ist, sondern Schadsoftware (z. T. unintendiert) in anderen Systemen wirksam wird.

Die Kodierung der Kategorien erfolgt gleichmäßig: Begonnen wird zumeist mit dem Start und (falls bekannt) Enddatum der Operation. Es folgen die betroffenen Receiver-Kategorien und Zielländer und, falls vorhanden, die attribuierten Initiatoren und deren Aufenthalts- bzw. Herkunftsländer mit den jeweiligen Regimetypen-Kategorisierungen anhand des Freedom House Index. Sodann werden alle den Attributionsprozess betreffenden Kategorien kodiert. Anschließend werden die im Rahmen der Operation potenziell zu identifizierenden Online-, und möglicherweise relevanten Offline-Konfliktgegenstände entsprechend des Konfliktbarometers des Heidelberger Instituts für internationale Konfliktforschung (HIIK) kodiert. Schließlich erfolgt die Bewertung der Operationsschäden anhand einer Intensitätsskala (siehe unten), die technische und sozio-politische Indikatoren inkludiert.

Bevor wir die bereits erwähnten Kategorien ausführlicher diskutieren, beschreiben wir nachfolgend detailliert den Kodierprozess und die dabei zur Anwendung gekommenen Prinzipien der Datenrecherche, Auswertung und Archivierung.

4.1. Zur Datenerhebung, Auswertung und Archivierung

Der Kodierprozess erfolgte mit einer teilautomatisierten Datenrecherche, die Push-Listen einschlägiger Quellen ebenso wie regelmäßige (wöchentliche) Webrecherchen rezenter Webseiten durch die MitarbeiterInnen, Hilfskräfte und ForschungspraktikantInnen beinhaltet. Ein solches, halbautomatisiertes Vorgehen wurde einer weitergehenden Automatisierung (zunächst) vorgezogen, weil entsprechende Tests zeigten, dass automatisierte(re) Verfahren – aufgrund entsprechender Algorithmen – einzelne Inzidenzkategorien nicht erfassten und zudem – aufgrund entsprechender Quellenüberschriften - zahlreiche Non-Events auswiesen. Mithin wurden halbautomatisiert gewonnene Quellen „analog" ausgebildete KodiererInnen ausgewertet. Zusätzlich wurden alle Einzelinzidenzen der Hilfskräfte und ForschungspraktikanntInnen durch die Projektmitarbeiterin gegenkodiert, um eine einheitliche Kodierlinie (Interkoderreliabilität) gewährleisten zu können. Die Kodierarbeit erfolgte im Regelfall mit etwa einem Jahr Zeitverzögerung, da Cyberoperationen oft erst mit großem Zeitverzug in der Öffentlichkeit bekannt werden und entsprechende (genauere) technische und politische Attributionen teilweise sogar erst Jahre später getätigt werden.[4] Ein „real-time" Kodierverfahren ist daher nicht nur sehr personalintensiv; es vermittelt auch immer nur ein „zeitlich verzögertes Lagebild", solange und sofern nicht sofort und öffentlich über die Cyberoperation berichtet wird. Solche kurzfristigen Lagebilder können wünschenswert sein, wenngleich aufwendig, wenn es um eine politikorientierte Anwendungsforschung geht. Für die Grundlagenforschung, die den Fokus stärker auf die Validität und Reliabilität anstatt auf die Aktualität und

[4] Insgesamt lässt sich allerdings auch feststellen, dass sich die Zeitspannen zwischen Inzidenz, Erstbericht und Attributionen verkürzt haben.

unmittelbare Handlungsorientierung der Daten legt, ist ein zeitverzögertes und sich wiederholendes, i.e. lernendes, Kodierverfahren von Cyberoperationen vorzuziehen. Dementsprechend wurden somit auch für bereits erfasste Fälle veränderte oder neu hinzugekommene Attributionsevidenzen auch noch zu einem späteren Zeitpunkt für den entsprechenden Fall aufgenommen, was eine weitere Herausforderung im Gegensatz zur traditionellen Konfliktforschung darstellt. Online-Quellen sind die primäre Informationsressource der Cyberkonfliktforschung. Um diese (oftmals schnell vergänglichen) Quellen längerfristig nutzen zu können, wurden die verwendeten Quellenlinks für die einzelnen Inzidenzeinträge im HTML-Format abgespeichert und somit nachhaltig archiviert. Bei der Einrichtung des HD-CY.CON sind wir auch der Vermutung nachgegangen, dass es Länder- bzw. kulturraumspezifische Attributionsprozesse geben könnte. In Abschnitt 4.6 gehen wir genauer darauf ein, inwiefern sich diese Vermutung als tragfähig erwies.

4.2. Technische & sozio-politische Relevanzkriterien

Die Kodierregeln des HD-CY.CON sehen für die Aufnahme einer Operation in die Datenbank vor, dass mindestens eine der drei Teile der CIA-Triade der Informationssicherheit (Confidentiality, Integrity, Availability) durch die Operation beeinträchtigt gewesen sein muss. Wenn in einer Quelle also lediglich „versuchte Infiltrationen" oder „Infizierungen" berichtet werden, oder aber das potenzielle Opfer öffentlich bestreitet, dass Daten in Folge der Operation abgeflossen seien, wurde die entsprechende Operation auch nicht in den Datensatz aufgenommen, insofern keine Drittparteien diese Behauptung aktiv angefochten haben. In diesem Projekt gehen wir davon aus, dass erhebliche Anreize für „Opfer" von Cyberangriffen bestehen, die Folgen der Angriffe herunter zu spielen, um bspw. den Börsenkurs eines Unternehmens nicht zu gefährden, bzw. ganz zu leugnen, um bspw. bestehende Verwundbarkeiten geheim halten zu können. Zweifeln jedoch DrittakteurInnen die Wahrscheinlichkeit oder Korrektheit dieser Aussagen nicht an, so wird das Bestreiten zur Grundlage für die Nicht-Kodierung.

Verletzte eine Operation eine der CIA-Komponenten, wurde geprüft, ob der Vorfall eines der folgenden Inklusionskriterien erfüllte:

Code	Subcode	Description
1		Attack conducted by nation state (generic "state-attribution" or direct attribution towards specific state-entities, e.g., intelligence agencies)
2		Attack conducted by non-state group/non-state actor with political goals (religious, ethnic, etc. groups)/undefined actor with political goals
	1	Attack conducted by a state-sponsored group ("cyber-proxies")
3		Targeted attack on political target; politicized
4		Targeted attack on political target; not politicized
5		Untargeted attack on political target; politicized
6		Targeted attack on non-political target; politicized
7		Untargeted attack on non-political target; politicized
8		Targeted attack on various targets; politicized
9		Untargeted attack on various targets; politicized
10		Targeted attack on (amongst others political) targets; not politicized.

Tabelle 1: Inklusionskriterien des HD-CY.CON.

Die Codes 1 - 2,1 beziehen sich auf die jeweiligen AngreiferInnen und deren Akteursprofile. Die übrigen Kategorien spezifizieren näher die Profile der Opfer. Die Kategorie 2,1 erfasst die für das Projekt zentrale Angreiferkategorie der Proxies. Wenn möglich, so wurden bei jedem Vorfall das betreffende Inklusionskriterium der AngreiferInnen- und der Opferseite kodiert. Bei einer fehlenden Attribution durch das Opfer oder Dritte ermöglichte in vielen Fällen jedoch ausschließlich das Profil der anvisierten Ziele die Aufnahme der Operation in den Datensatz.

Operationen, in denen weder der Angreifer, noch das Opfer politische AkteurInnen oder politisch motiviert waren, z. B. cyberkriminelle Operationen, wurden dann in den Datensatz aufgenommen, wenn die Operation nachträglich politisiert wurde. Politisierung findet dann (laut Kodierhandbuch) statt, wenn ein Akteur aus dem politischen System (bspw. aus dem Zielland oder einem Drittstaat) durch einen Sprechakt oder eine Handlung (z.B. das Einsetzen einer Untersuchungskommission) diesen Vorfall auf die politische Agenda setzt, bzw. der Operation eine politische Bedeutung zuweist, z.B. Einschüchterung.

4.3. AngreiferInnen im Cyberspace

Bei der Kodierung unterschiedlicher Typen von CyberangreiferInnen erweitert und spezifiziert der HD-CY.CON die bestehenden Datensätze DCID und CFR Tracker in mehrerlei Hinsicht: Erstens erfasst er nicht nur staatliche oder dem Staat zugeschriebene AkteurInnen, wie nichtstaatliche Cyberproxies im staatlichen Auftrag, sondern auch genuin nichtstaatliche HackerInnen, wie z.B. Anonymous oder auch patriotische Hackergruppen ohne direkte staatliche Affiliation. Zweitens verwendet HD-CY.CON keine generische „Catch-All"-Kategorie im Sinne einer allgemeinen staatlichen Beteiligung am Angriff. Vielmehr unterscheiden wir zwischen allgemein/direkt-staatlichen Operationen und solchen durch staatliche AkteurInnen initiiert, unterstützt oder auf andere Weise gesponsert, jedoch laut Attribution von Proxy-AkteurInnen durchgeführten Vorfällen. Drittens unterscheiden wir bei der Kodierung zwischen Fällen in denen ein Proxy konkret als Stellvertreter, z. B. durch das Zielland, benannt wurde und solchen Fällen, in denen ein Proxy nicht direkt durch das Opfer benannt wurde, zum Zeitpunkt der Attribution jedoch bereits ein Konsens (zumeist in der IT-Sicherheits-Community) über die, zumindest vorherige zeitweilige, Proxy-Rollenübernahme existierte. Diese (kleinteilige) Differenzierung erlaubt es uns der Frage nachzugehen, wann und welche attribuierenden AkteurInnen trotz bereits existierender vorheriger Benennungen eines Advanced Persistent Threat (APT) als Stellvertreter eines Staates in einzelnen Fällen von einer wiederholten Attribution staatlich-gesponserter Proxy zurückschrecken, bzw. diese unterlassen.

Eine gewichtige Besonderheit des HD-CY.CON-Datensatzes ist die getrennte Erfassung von politischen und technischen Attributionen. So sind für die technische Attribution seitens IT-Unternehmen gesonderte „Initiator Category" und „Initiator Country"-Spalten angelegt, um deren Verantwortungszuweisung von denen politischer AkteurInnen zu unterscheiden. Diese heißen im Datensatz „Attribution IT-security community (initiator category)" sowie „Attribution IT-security community (initiator country)". Liegt für einen Fall nur eine Attribution der IT-Community vor, ergibt sich die Kodierung der Kategorien „Initiator Category" und „Initiator Country" automatisch aus diesen beiden letztgenannten Kategorien.

In der Gruppe der nichtstaatlichen AkteurInnen unterscheidet der HD-CY.CON zudem zwischen unterschiedlich motivierten Akteursgruppen, wie sie in Tabelle 2 unter Code 3. und 4. subsumiert werden.

Code	Subcode	Description
0		Unknown - not attributed
1		State
2		Non-state actor, state sponsorship suggested
	1	Non-State-Group, state-sponsorship suggested (widely held view, but not invoked in this case)
3		Non-state - group
	1	Ethnic Actors
	2	Religious Actors
	3	Hacktivist(s)
	4	Criminal(s)
	5	Terrorist(s)
	6	Other Actors (e.g., private technology companies, hacking for hire groups without state affiliation or research entities)
4		Individual Hacker(s)
5		Other

Tabelle 2: AngreiferInnen-Kategorien im HD-CY.CON

4.4. Ziele im Cyberspace

Neben Staaten treten auch immer häufiger zivilgesellschaftliche AkteurInnen als Ziele von bösartigen Cyberoperationen in Erscheinung. Im HD-CY.CON kodieren wir beide Akteurszielgruppen als auch deren jeweiligen geografischen Ursprung entsprechend ihres ISO-Country-Codes. Im Kodierhandbuch unterscheiden wir zwischen politischen und nichtpolitischen AkteurInnen und differenzieren diese in folgenden übergeordneten Kategorien weiter aus:

1. Politische/staatliche AkteurInnen,
2. Supranationale/internationale (politische) Organisationen,
3. Kritische Infrastrukturen,
4. Soziale Gruppierungen,
5. Unternehmen,
6. Enduser,
7. Medien/Journalisten und
8. Wissenschaft/Forschung.

In den übergeordneten Kategorien Politische/staatliche AkteurInnen (1), Kritische Infrastrukturen (3) und Soziale Gruppierungen (4) bietet das Kategoriensystem zudem weitere Spezifikationsmöglichkeiten. So werden bspw. die Identifikation und Analyse besonders bedrohter Akteursgruppen über Zeit, bspw. kritische Infrastrukturen[5], und die Offenlegung einer graduellen Veränderung zwischen diesen ermöglicht. Durch die Spezifikation von Untersektoren können wir deshalb, wie im Falle der Covid-19-Pandemie, erkennen, ob und inwiefern der Gesundheitssektor verstärkt in den Fokus staatlicher und nichtstaatlicher Cyberangriffe gerät.

Prinzipiell sollte die sektorenspezifische Kodierung es auch erlauben, die Wirkung von Regulations- oder Sanktionsprozessen zu analysieren: Würden bspw. digitale Wahlsysteme als kritische Infrastruktur deklariert, könnte untersucht werden, ob die Abschreckungs- und Resilienzin-

[5] Die aufgelisteten Teilbereiche kritischer Infrastrukturen stellen eine Art kleinsten, gemeinsamen Nenner der nationalen Designationen in diesem Bereich dar und müssten entsprechend veränderter Definitionen über Zeit aktualisiert werden.

strumente auch für diesen neuen Bereich ihre Wirkung entfalten. Wichtig ist bei diesem Beispiel abermals zu betonen, dass der HD-CY.CON lediglich Aussagen über öffentlich berichtete Vorfälle treffen kann und es erhebliche Anreize für Wahlbehörden geben kann, eine Kompromittierung erst spät(er) zu berichten, u.a. bspw. um den eindringenden Akteur in seiner Vorgehensweise zu beobachten und erst nach einiger Zeit zu überführen.

Code	Subcode	Description
0		Unknown
1		State institutions / political system
	1	Government / ministries
	2	Legislative
	3	Civil service / administration
	4	Judiciary
	5	Military
	6	Police
	7	Intelligence agencies
	8	Political parties
	9	Election infrastructure/related systems
	11	Other (e.g., embassies)
2		International/supranational organization
3		Critical infrastructure
	1	Energy
	2	Water
	3	Transportation
	4	Health
	5	Chemicals
	6	Telecommunications
	7	Food
	8	Finance
	9	Defence industry
4		Social groups
	1	Ethnic
	2	Religious
	3	Hacktivist
	4	Criminal
	5	Terrorist
	6	Human Rights Organizations/Activists
	7	Political Opposition/Dissidents/Expats
	8	Other (e.g., NGOs with political goals)
5		Commercial
6		End user(s)
7		Media
8		Science
9		Other

Tabelle 3: Zielkategorien im HD-CY.CON.

4.5. Ein mehrdimensionaler Ansatz zur Erfassung von Attribution

Der nächste Schritt im Kodierprozess, nachdem die entsprechende Interaktions-/Konfliktdyade beschrieben wurde, ist die detaillierte Beschreibung/Einordnung der jeweiligen Attributionsmerkmale. Hierzu zählen folgende Kategorien:

- Attribution Basis
- Attribution Type
- Attribution Year
- Temporal Sequence Attribution

Die erste Kategorie, Attribution Basis, erfasst, welche(r) Akteur(e) oder welche Institution(en) die erfasste(n) Attribution(en) vorgenommen hat/haben. Da der HD-CY.CON auf möglichst umfassende Attributionsbewertungen abzielt, sind hier Mehrfachkodierungen möglich. Tabelle 4 listet die Attributionsquellen auf:

Code	Description
0	Unknown - not attributed/Media-based attribution
1	Receiver attributes attacker
2	IT-security community attributes attacker
3	Attacker confirms
4	Contested attribution
5	Attribution by Third-Party (e.g., state entity by a foreign state or scientific laboratories)
6	Attribution by Receiver Government/State Entity

Tabelle 4: Die Kategorie der Attribution Basis im HD-CY.CON.

Liegt eine Attribution für einen Fall vor und wurde gleichzeitig eine „0" bei Attribution Basis kodiert, steht diese Kodierung für Medien/JournalistInnen als Attributionsquelle. Die dritte Kategorie „Attacker confirms" wird zumeist dann kodiert, wenn HacktivistInnen sowie patriotische HackerInnen selbst über ihre Angriffe im Sinne einer „voluntary attribution" berichten (Poznansky und Perkoski 2018). Dies betrifft etwa Mitteilungen auf Social-Media-Kanälen oder reklamierte DDoS-Attacken auf Webpages der Kontrahenten, z.B. die Regierungsseiten eines Staates, der sich häufig in einer „enduring rivalry" mit dem Heimatstaat der HackerInnengruppe befindet (Goertz und Diehl 1992).

Die vierte Ausprägung, „contested attribution", wird dann zusätzlich neben den Codes „2" und „6" mit „4" kodiert, wenn die politischen und technischen Verantwortungszuweisungen signifikant auseinandergehen. Sie wird indes nur dann kodiert, wenn es einen aktiven Widerspruch gibt: das alleinige Anzweifeln einer IT-Firma, ob die Attribution einer Regierung wirklich in der veröffentlichten Form zum jeweiligen Zeitpunkt bereits vorgenommen werden kann, wird nicht als „contested" gewertet.

Für die fünfte Kategorie der „Third-Parties" ist zu erläutern, dass es sich hierbei erstens um einen Geheimdienst/Sicherheitsbehörde eines Drittstaats, etwa um eine Attribution des FBI handeln könnte, welcher im Falle einer Cyberoperation Attributionen vornimmt, in die keine US-AkteurInnen involviert sind; zweitens kann es sich um Attributionen handeln, die von einem zivilgesellschaftlichen Akteur/Institut (z.B. Citizen Lab in Toronto) oder drittens von einer Privatperson ausgehen, wie dem Whistleblower Edward Snowden.

HD-CY.CON erfasst in Ergänzung zur Kategorie „Attribution Basis" auch die Art und Weise der Attribution, also in welcher Form diese stattgefun-

Code	Description
0	Attribution type unclear
1	Self-attribution in the course of the attack (e.g., via defacement statements on websites)
2	Media report (e.g., Reuters makes an attribution statement, without naming further sources)
3	Direct statement in media report (e.g., Reuters article cites the attribution statements by a person) / self-attribution via social media
4	Anonymous statement in media report (e.g., Reuters article cites the attribution statements of unnamed officials, or persons with knowledge into the matter etc.)
5	Technical report (e.g., by IT-companies, Citizen Lab, EFF)
6	Political statement / report (e.g., on government / state agency websites)
7	Indictment/sanctions / arrests (by state authorities) / lawsuit (by private actors)
8	Statement in media report and political statement/technical report
9	Statement in media report and indictment / sanctions
10	Political statement/report and indictment / sanctions

Tabelle 5: Die Kategorie des Attribution Types im HD-CY.CON

den hat. Tabelle 5 listet die dabei möglichen Ausprägungen sowie Kombinationsmöglichkeiten:

Jeder kodierten Attribution Basis wird im Datensatz also auch ein Attribution Type zugeordnet. Die Kombinationsmöglichkeiten von 8-10 reflektieren dabei, dass auch ein und derselbe Attributionsakteur unterschiedliche Attributionstypen, womöglich auch in zeitlicher Sequenzierung, nutzen kann.

In der Kategorie des Attribution Year werden jene Fälle erfasst, in welchen auf der AngreiferInnenseite eine staatliche Involvierung attribuiert wurde (Initiator Categories 1; 2 und 2,1), für das Jahr der Attribution. Falls dieser Attribution auch noch ein Indictment/Sanktion/ Verhaftung oder auch private Anzeige nachfolgte, wird deren Veröffentlichungs-/Durchführungsjahr ebenfalls separat gelistet.

Die Kategorie der Temporal Attribution Sequence gibt an, welche Zuweisung im Falle einer politischen und technischen Attribution zuerst erfolgte. Aufgrund der teilweise sehr komplexen Quellenlage, etwa durch zahlreiche Querverbindungen und sich aufeinander beziehende Inhalte, ließ sich diese Kategorie nicht immer mit hoher Konfidenz kodieren.

4.6. Unterschiedliche Sprachwelten, unterschiedliche Attributionsrealitäten?

Eine wichtige Ausgangsfragestellung des Projektes war, ob es Länder- oder Sprachraum spezifische „Attributionswelten“ gibt, d.h. konkret ob insbesondere in der russisch- und chinesischsprachigen Welt andere Cyberoperationen erfasst und attribuiert werden oder ob jene aus westlichen Berichten anders erfasst werden. Diese Sprachen wurden ausgewählt, da die Russische Föderation und Volksrepublik China unter den autokratischen Regimen die dominantesten und offensivsten CyberakteurInnen sind und ihre Regierungen in unserem liberalen Erklärungsmodell erhebliche Anreize besitzen könnten, den innerstaatlichen Attributionsdiskurs in ih-

rem Sinne zu lenken. Für die Jahre 2013 bis 2016 wurden deshalb vorab in ca. 50 Cybervorfällen russisch- und chinesischsprachige Quellen kodiert und auf mögliche abweichende Berichterstattung und Bewertungsunterschiede zu englischsprachigen Quellen hin untersucht.

Die Befunde dieses „Pre-Tests" zeichneten folgendes Bild: Erstens berichteten Medien und IT-Sicherheitsfirmen in beiden Sprachen kaum oder gar nicht über Cyberoperationen, die in westlichen Berichten keine Erwähnung fanden; der Datensatz konnte also nicht um vorher nicht erfasste Operationen erweitert werden. Zweitens fanden die russisch- und chinesisch-sprachigen KodiererInnen heraus, dass Medien/Berichte in beiden Staaten oft englischsprachige Quellen paraphrasierend oder wortgleich wiedergeben, wenn weder China noch Russland selbst beteiligt sind. Im quantitativen Vergleich berichteten russische AkteurInnen noch häufiger über Cyberoperationen als chinesische. Dies könnte auf die vergleichsweise größere Offenheit der russischen Medienlandschaft sowie der digitalen Informationssphäre rund um das RUNET zurückzuführen sein, die sich vom stark abgeschotteten chinesischen Informationsraum (bislang) noch unterscheidet (Griffiths 2019).

Drittens zeigte die Auswertung der russischsprachigen Quellen deutliche Anzeichen für eine Politisierung von Cyberangriffen, die sich in englischsprachigen Quellen so (stark) nicht identifizieren ließ. Insgesamt überstiegen die Kosten der Pilotuntersuchungen aber den begrenzten Nutzen einer dauerhaften Kodierung russisch- und chinesischsprachiger Quellen, sodass wir in der Folge darauf verzichtet haben. Es ist indes nicht auszuschließen, dass eine fortwährende Fragmentierung des Internets in Zukunft auch stärker auf die Berichterstattung über Cyberoperation in dann jeweils entstehenden (abgeschotteten) Cyberräumen wirken könnte (Drake et al. 2016)

4.7. Cyberoperationen: Spionage, Disruption und Hijacking

Die Kodierung der technischen Eigenschaften des Angriffs beginnt mit der Kategorie des Incident Types. Der HD-CY.CON unterscheidet dabei zwischen Data Theft, Disruption sowie Hijacking. Diese Unterscheidung ist besonders relevant für die vergleichende Analyse autokratischer Cyberproxies: Führen chinesische und russische Cyberproxies regelmäßig unterschiedliche Cyberoperationen durch? Falls ja, wie lässt sich diese Varianz aus Sicht der innerstaatlichen und internationalen Sicherheitsinteressen des jeweiligen Regimes erklären?

Die Kategorie „Data Theft" kann spezifischer als Doxing kodiert sein: In solchen Fällen wurden Daten nicht nur elektronisch „gestohlen", sondern in der Abfolge durch die TäterInnen selbst, deren AuftraggeberInnen oder Dritte, i.e. Whistleblower-Plattformen wie Wikileaks, veröffentlicht, wobei dies auch in manipulierter Form geschehen kann (sogenannte „Tainted Leaks", Hulcoop et al. 2017). Das wohl bekannteste Beispiel für eine solche Hack-and-Leak-Operation stellt der Diebstahl und die Veröffentlichung von sensiblen Daten des Democratic National Committee im Vorfeld der US-Präsidentschaftswahlen 2016 dar. Dieser Vorfall verdeutlichte die Brisanz sogenannter „Cyber-enabled Information Operations" (Lin 2019).

Disruption meint hingegen in erster Linie solche Operationsformen, die Zielsysteme in ihrer Funktionsweise stören, zumeist deren Availability. Die häufigste Form der Disruption-Kategorie sind bislang DDoS- oder auch Defacement-Angriffe. Ihr Ziel ist es, Webseiten lahm zu legen und darauf eigene, ideologisch aufgeladene Inhalte zu platzieren. Hijacking bezeichnet ein technisches Vorgehen, das es den AngreiferInnen prinzipiell erlauben würde durch die erlangten, tiefergehenden Zugriffsrechte auf die Zielsysteme weitere, schwerwiegendere Funkti-

onsstörungen oder aber auch Sabotageakte, i.e. dauerhafte Zerstörung von Hard- und Software, vorzunehmen. Besondere Brisanz erhält Hijacking verbunden mit Disruption, wenn die Operation auf die Steuerungsanlagen kritischer Infrastrukturen gerichtet ist. So hat der Computer-Wurm Stuxnet 2010 eindrucksvoll gezeigt, welche physischen Schäden mit Hilfe von (sehr) sophistizierten (mehrstufigen) Hijacking-Operationen etwa an den Zentrifugen einer Atomanlage verursacht werden können (vgl. Farwell und Rohozinski 2011). Hijacking mit Misuse kann neben einer Disruption, die durch Hijacking erst ermöglicht wurde, jedoch auch im Verbund mit Datendiebstahl (Data Theft) auftreten. Hijacking wird hier genutzt, um an besonders gut geschützte Daten des anvisierten Opfers zu gelangen.

Für solche Fälle, in denen ein erfolgreiches Hijacking ohne Misuse durch Data Theft und/oder Disruption erkennbar ist, diskutiert die Forschung die potentiellen Eskalationsrisiken einer solchen Hjacking-Operation: Wertet das Opfer einer erfolgreichen Infiltration schon die Möglichkeit einer späteren Ausnutzung der Zugriffsrechte seines Systems als „Angriff", dann wären präventive oder reaktive Maßnahmen die wahrscheinliche Folge, ein „Cybersecurity Dilemma" entstünde (Buchanan 2017). Das Errichten sogenannter „Beachheads" (Buchanan und Cunningham 2020, S. 66) in fremden Systemen, die (zunächst) ungenutzt bleiben, könnte so zu einer erheblichen Eskalation in der jeweiligen Konfliktdyade, bspw. im Offline-Bereich, beitragen.

Einen (Kodier-) Sonderfall stellt Hijacking ohne Misuse in jenen Fällen dar, in denen eine Bank infiltriert wurde, jedoch keine Daten gestohlen und auch kein Service in seiner Funktionsweise gestört wurde, sondern ohne Autorisierung eine Zahlung in Auftrag gegeben wurde. Diese Form des Missbrauchs lässt sich im HD-CY.CON weder über Data Theft, noch über Disruption adäquat abbilden. Solche Fälle werden im HD-CY.CON daher nur durch Hijacking ohne Misuse bewertet.

4.8. Eine Intensitätsskala zur Bewertung unterschiedlicher Cyberoperationen

Der HD-CY.CON nimmt, ähnlich wie der DCID, eine Intensitätsbewertung der erfassten Operationen vor. Diese erfolgt auf der Grundlage der technischen Bewertung der kodierten Incident Types und der Erfassung der berichteten physischen Effekte/Schäden der Cyberoperation. Die Summe dieser einzelnen Teilwerte wird dann und insoweit mit einem Target Effect Multiplier multipliziert, insofern die Cyberoperation eine „sehr große, politische Bedeutung" erlangt.

Der Intensitätsbemessungsprozess beginnt für einen Fall mit Data Theft mit der Bewertung der Sensitivität, bzw. Klassifikation der abgegriffenen Daten aus Sicht des jeweiligen Opfers. Diese können entweder mit dem Wert 1 oder 2 bewertet werden (Tabelle 6).

Auch bei der Spezifikation der Sensitivität der gestohlenen Daten gilt, dass gerade geschädigte AkteurInnen Anreize haben könnten, die Schwere eines Angriffs und hier vor allem die Sensitivität der Daten herunter zu spielen. Da die Einschätzungen der Angriffseffekte durch die Opfer (oft) von Dritten, z.B. IT-ExpertInnen oder anonym bleibenden InsiderInnen, angezweifelt werden, können die Angaben der Geschädigten (in manchen Fällen) mit unabhängigeren Einschätzungen verglichen werden.[6]

Im Falle von Disruptionen wird primär die zeitliche Dauer der Funktionsstörung bewertet (Ta-

[6] Grundsätzlich sind IT-Sicherheitsunternehmen nicht als „unabhängige Sachverständige" anzusehen, weil sie in der Regel durch die Bereitstellung von IT-Sicherheitsdienstleistungen mittel- oder unmittelbar von ihren eigenen Gefahreneinschätzungen, oder jenen ihrer MitwettbewerberInnen, profitieren können, vgl. Weiss 2021.

belle 7). Den Großteil der erfassten Vorfälle machen hier niedrigschwellige DDoS-Operationen aus. Diese dauern zumeist nur wenige Stunden, sodass ein Schwellenwert von mehr als 24 Stunden für die Intensitätsabstufung gewählt wurde.

Sodann werden zwei Formen von Hijacking, ohne oder mit erfolgtem Missbrauch, unterschieden (Tabelle 8). Wird in diesen Fällen eine schwerwiegende Intensität („2") festgestellt, dann wird regelmäßig auch noch eine der beiden anderen Incident Type-Kategorien kodiert, welche die Art und Form des Missbrauchs bezeichnen.

Um die Bewertung des ungewichteten Intensitätswert abzuschließen, gilt es zuletzt zu prüfen, ob der Vorfall direkte physische Schäden, wie im Falle von Stuxnet hervorgerufen hat. Diese Schäden werden nochmals im Hinblick auf ihre räumliche und zeitliche Wirkung bewertet (Tabelle 9). Ist diese Bewertung erfolgt, werden die Teilwerte der Incident Types sowie der ermittelten physischen Schäden (bislang wurde ein Großteil der Fälle hier mit „0" kodiert) aufsummiert, sodass sich ein ungewichteter Intensitätswert auf einer Skala von „1" bis „10" ergibt.

Um die Gewichtung der Intensitätsbewertung vornehmen zu können, bedarf es abschließend der Bewertung der gesamtgesellschaftlichen Salienz der Cyberoperation. Der Target/Effect-Multiplier unterscheidet Operationen mit moderater bis hoher politischer Relevanz (Wert: 1) von Angriffen mit sehr hoher/extremer Relevanz (Wert: 2), wobei Operationen, die die kritische Infrastruktur von Staaten oder konventionelle defensive/offensive Militärkapazitäten eines Landes beeinträchtigen oder gar beschädigen, mit einem Wert von 1,5 gewichtet werden (Tabelle 10).

Kritische Infrastrukturen, als auch Militäreinrichtungen sind regelmäßig Ziele konventioneller Offline-Konflikte mit Gewaltanwendung. Indem wir Angriffe auf kritische Infrastruktur mit einem Effekt-Multiplier-Wert von 1,5 belegen, bilden wir die kinetische Wirkung dieser Angriffsart ab, die sich der Wirkung konventioneller Angriffe annähert. Operationen, die keine kinetischen Effekte entfalten, und das ist bislang die Mehrzahl der im HD-CY.CON kodierten Operationen, werden mit einem Effect-Multiplier-Wert von 1 multipliziert. Es gibt nur wenige Fälle, insgesamt vier, die einen Effect-Multiplier von 1,5 aufweisen. Dazu gehören u.a. der Stuxnet-Angriff (2010) sowie die Stromausfälle in der Ukraine (2015 & 2016), da hier weitflächig die kritische Stromversorgungsleistung für größere Bevölkerungsteile durch einen Cyberangriff (zeitweise) beeinträchtigt wurde.

Der Gesamtintensitätsdurchschnittswert des HD-CY.CON liegt daher bislang bei einer niedrigen Intensität von 1,85 (2000-2019). Auch wenn man nur den Durchschnitt der Operationen mit staatlicher Beteiligung auf der AngreiferInnenseite ermittelt, ist der Wert geringfügig erhöht (2,37). Auf zeitlicher Ebene lassen sich dabei keine signifikanten Muster hinsichtlich Intensitätssteigerungen oder -abfällen feststellen.[7]

[7] Der HD-CY.CON verzeichnet auch physisch Verletzte/Todesopfer in direkter Folge einer Cyberoperation. Bislang wurde aber keine derartige Operation verzeichnet. Im Fall der Ransomware-Operation auf das Düsseldorfer Universitätskrankenhaus (September 2020) kamen Ermittlungen im Nachgang zu dem Ergebnis, dass die im Zusammenhang mit einem umgeleiteten Rettungswagen verstorbene Patientin sehr wahrscheinlich auch auf dem Weg oder im eigentlichen Zielkrankenhaus verstorben wäre (Ralston 2020).

Code	Description
0	none
1	For political/military targets: non-classified information (Incident scores 1 point in intensity) For private/commercial targets: non-sensitive information (Incident scores 1 point in intensity)
2	For political/military targets: classified information (Incident scores 2 points in intensity) For private/commercial targets: sensitive information (Incident scores 2 points in intensity)

Tabelle 6: Intensitätsbewertung der Data Theft Kategorie

Code	Description
0	none
1	Short-term disruption (Incident scores 1 point in intensity) (< 24 h)
2	Long-term disruption (Incident scores 2 points in intensity) (> 24 h)

Tabelle 7: Intensitätsbewertung der Disruption Kategorie

Code	Description
0	none
1	Hijacking, not used - empowerment (Incident scores 1 point in intensity)
2	Hijacking, system misuse (Incident scores 2 points in intensity)

Tabelle 8: Intensitätsbewertung der Hijacking Kategorie

Code	Description
0	none
1	Local effects (Incident scores 1 point in intensity)
2	Widespread effects (Incident scores 2 points in intensity)
0	none
1	Short duration (Incident scores 1 point in intensity)
2	Long lasting effects (Incident scores 2 points in intensity)

Tabelle 9: Bewertung der physischen Effekte (räumlich & zeitlich)

Code	Description
1	Moderate - High political importance
2	Very high political importance (e.g., critical infrastructure, military) - intensity multiplied by 1.5

Tabelle 10: Der Target/Effect- Multiplier

4.9. Verschränkungseffekte zwischen Online- und Offline-Konflikten

Die systematische Messung von Konfliktintensitäten erlaubt, neben anderen Charakteristika des Heidelberger Datensatzes, auch die Untersuchung der Schnittstelle zwischen On- und Offlinekonfliktdynamiken. Bislang konnte die Forschung hier keinen klaren oder gar einseitigen Wirkungszusammenhang in die eine – Onlinekonflikte schüren oder dämpfen Offlinekonfliktdynamiken – oder andere Richtung feststellen (Maness und Valeriano 2016). Gleichwohl erscheint es weiterhin plausibel einen wie auch immer gearteten Zusammenhang zu vermuten, denn schon vor einigen Jahren wurde festgestellt, dass Cyberkonflikte - trotz der grenzüberschreitenden technischen Möglichkeiten - oftmals regionalen Konfliktmustern zu entsprechen scheinen (Valeriano und Maness 2014).

Für eine verschränkte Konfliktintensitätsmessung von Off- und Onlinedynamiken bietet es sich zunächst an, die Intensitätswerte des HDCY.CON mit der granularen Intensitätsmessung des Konfliktbarometers des HIIK zu verknüpfen. Das Konfliktbarometer unterscheidet fünf Stufen zwischen gewaltlosen (1-2) und gewaltsamen (3-4) Konflikten bis hin zum Krieg (5). Sodann haben wir die Kategorisierung von Konfliktgegenständen der HIIK-Systematik entnommen und um einen weiteren „cyber-spezifischen" Konfliktgegenstand ergänzt (Tabelle 11). Dieser Gegenstand umfasst Cyberoperationen, die sich direkt auf Vorfälle oder Handlungen im Cyberraum beziehen, bspw. DDoS-Angriffe von HacktivistInnen gegen ein nationales Gericht, welches Online-Zensur-Maßnahmen verhängt hat. In diesem konkreten Fall würde zusätzlich der Konfliktgegenstand „System/Ideology" kodiert werden.

In vielen Fällen, vor allem bei Data-Theft-Operationen, kann (lange Zeit) keine seriöse Aussage über den zu Grunde liegenden Konfliktgegenstand getroffen werden. Anders hingegen verhält es bei der Mehrzahl der verzeichneten DDoS- oder Defacement-Operationen, die von HacktivistInnen oder patriotischen HackerInnen ausgehen, denn diese bekennen sich nicht nur oft selbst als TäterInnen, sondern nennen auch

Code	Description
0	Unknown
1	System/Ideology
2	National Power
3	Autonomy
4	Territory
5	Subnational Predominance
6	Resources
7	International Power
8	Decolonization
9	Secession
10	Cyber-specific
11	Other

Tabelle 11: Online-Konfliktgegenstände entsprechend der HIIK-Taxonomie*

**Anmerkung: Der HIIK-Konfliktgegenstand der „Dekolonialisierung" wurde bewusst ausgelassen, da diesem eine geringere Salienz für Cyberoperationen unterstellt wurde.*

häufig die Gründe für ihre Tat. Ähnliches gilt für Cyberspionage-Operationen, denn hier kann oftmals plausibel auf den Konfliktgegenstand „International Power“ (andere Staaten) und/oder „National Power“ (Dissidenten/ Oppositionelle) geschlossen werden.

Wurde ein Konfliktgegenstand auf der Cyberebene kodiert, so kann im HIIK-Konfliktbarometer des betreffenden Operationsstartjahres überprüft werden, ob für dieselbe Konfliktdyade ein Offline-Konflikt mit gleichem Konfliktgegenstand kodiert wurde. Für manche Dyaden erfasst das HIIK-Barometer mehrere Konfliktgegenstände, sodass sich nicht notwendigerweise alle auf der Cyberebene wiederfinden lassen müssen. Stimmt mindestens ein Off- und Onlinekonfliktgegenstand überein, werden sie als solche im HD-CY.CON kodiert. Auffallend ist, dass für sog. „Enduring Rivalries“ (Indien vs. Pakistan, Südkorea vs. Nordkorea, Iran vs. Israel oder auch Armenien vs. Aserbaidschan) diese Verschränkungen zwischen der Online- und der Offline-Konfliktebene besonders häufig verzeichnet werden mussten.

Die insgesamt niedrigen bis moderaten Konfliktintensitäten in Cyberkonflikten werden seit geraumer Zeit intensiv diskutiert (s. Maschmeyer 2021). Die Befunde des HD-CY.CON-Datensatzes verdeutlichen, dass niedrige Intensitäten nicht in allen Dyaden gleichermaßen und über Zeit stabil gegeben sind; so lässt sich bspw. für russische Cyberoperationen zeigen, dass disruptive Techniken nicht nur vorhanden sind, sondern auch parallel zum Offline-Konflikt in der Ukraine eingesetzt wurden. Ob und inwieweit solche Techniken „getestet“ wurden (Cerulus 2019), um sie auch gegen (konventionell) potentere Gegner einzusetzen, ist umstritten.[8]

[8] Ein ähnliches Vorgehen wurde bereits für chinesische Cyberoperationen gegen taiwanesische Ziele behauptet (Gold 2013).

5. Geheimhaltung & Verschleierung: Autokratische & demokratische Cyberproxies

Im folgenden Kapitel beschreiben und analysieren wir die im HD-CY.CON erfasste Cyberproxy-Nutzung durch demokratische und autokratische Regime. Wir ließen uns dabei von der Frage anleiten, ob und auf welche Weise die jeweiligen Regierungen nichtstaatliche CyberakteurInnen einsetzen, um die eigene Verantwortlichkeit zu verschleiern. Auf der Grundlage unseres liberalen Erklärungsmodells erwarteten wir, dass autokratische Regierungen unterschiedliche Typen von nichtstaatlichen Cyberproxies für offensive Operationen nutzen, während demokratische Regierungen Cyberproxies für defensive Zwecke, i.e. technische Attributionen, einsetzen. Trotz dieser binären Unterscheidung galt es zugleich potenzielle Varianzen innerhalb der beiden Regimetypen ebenfalls in den Blick zu nehmen. Auf Seiten der Autokratien werden daher zunächst allgemeine Kennzahlen des HD-CY.CON präsentiert, um die getroffene Fallauswahl für den anschließenden Vergleich zu begründen.

5.1 Autokratische Cyberproxies im HD-CY.CON: Eine Übersicht

Mit insgesamt 309 verzeichneten Fällen stellen Proxies (staatlich-gesponserte AkteurInnen) nach HacktivistInnen/patriotischen HackerInnen (465 Fälle) die am zweithäufigsten attribuierte AngreiferInnenkategorie im HD-CY.CON dar. Abbildung 1 zeigt, dass sich die Annahme des Projektes, in erster Linie seien autokratische Staaten für den Einsatz nichtstaatlicher AkteurInnen mit offensivem Hackingauftrag verantwortlich, bestätigt. Das Ausmaß des „autokratischen Sponsoring" kann indes erheblich variieren. Es reicht in der von Jason Healey vorgeschlagenen Kategorisierung der staatlichen Verantwortlichkeit für Cyberoperationen von StellvertreterInnen von „state-ignored" bis hin zu „state-integrated" Operationen (Healey 2011).

Nur in vier Fällen von „state-sponsored" Operationen zeichneten sich demokratische Staaten als verantwortliche „Benefactors", dabei handelte es sich ausschließlich um Hackingoperationen der Gruppierung DarkHotel, die der südkoreanischen Regierung in der Konfliktdyade mit Nordkorea zugeordnet wird (Greenberg 2020). Deutlich erkennbar ist in Abb. 1 auch, dass die Anzahl offensiver Operationen durch autokratische Regime nach 2010 ansteigt und sich (bis 2016) auf moderatem Niveau stabilisiert.

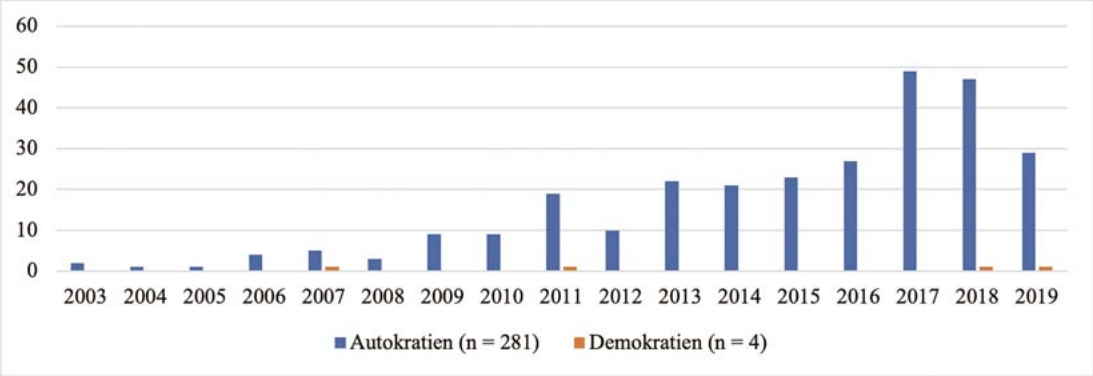

Abbildung 1: Offensive Cyber-Proxy-Operationen: Regimetyp des attribuierten „Sponsors"[9]

[9] Die Abbildungen und Tabellen entstammen der 2022 erscheinenden Dissertation der Projektmitarbeiterin Kerstin Zettl-Schabath (2022b).

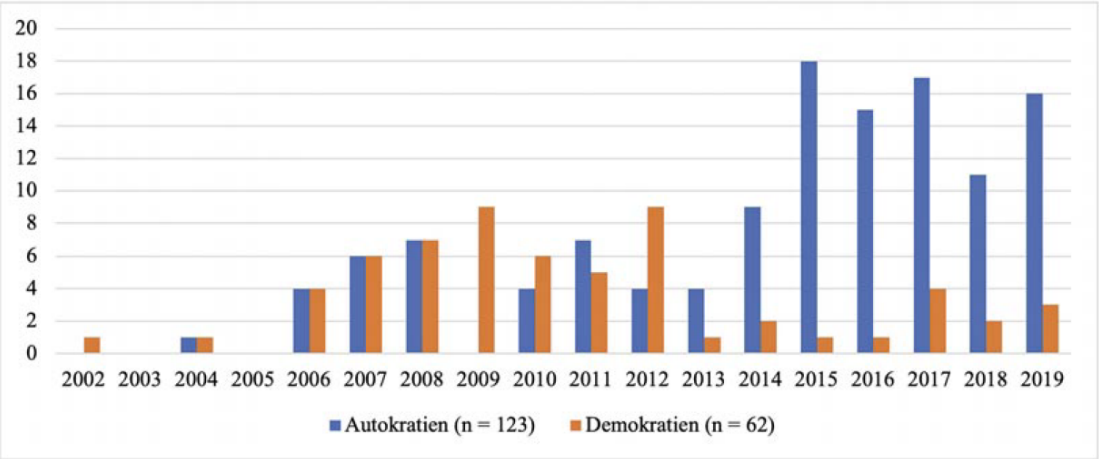

Abbildung 2: Allgemein/direkt-staatliche Operationen entsprechend des Regimetyps der AngreiferInnen

Nimmt man die Anzahl aller allgemein oder direkt-staatlich attribuierten AkteurInnen für Cyberoperationen in den Blick, dann ist das Verhältnis zwischen Autokratien und Demokratien deutlich ausgeglichener. Zwar rangieren hier im Gesamtzeitraum autokratische Regierungen mit insgesamt 123 Operationen vor demokratischen Regierungen, denen lediglich 62 öffentlich bekannt gewordene Cyberoperationen zugeschrieben wurden (Abbildung 2). Eine prinzipielle Zurückhaltung demokratischer Staaten im Cyberraum lässt sich daraus allerdings nicht ableiten.

Abbildung 3 veranschaulicht, dass sich die Mehrzahl der 281 im HD-CY.CON verzeichneten autokratischen Cyberproxyoperationen gegen Ziele in demokratischen Staaten richten. Diese Operationen zielen vor allem auf die USA und weitere westliche Industrienationen, deren nationale Institutionen sowie internationale Organisationen ab. Im Zeitverlauf wird allerdings seit 2013 erkennbar, dass es zunehmend auch zu Angriffen zwischen autokratischen Regimen kommt.

Für unsere Vergleichsstudie wählten wir jene autokratischen Staaten aus, die am häufigsten Cyberproxies einsetzen (most likely case), um zu ergründen, ob und inwiefern unterschiedliche autokratische Subtypen auch unterschiedliche StellvertreterInnentypen nutzen (Tabelle 12).

Unter den Nutznießern („benefactors“) der Autokratien zugeschriebenen Cyberproxyoperationen nimmt die Volksrepublik China die Spit-

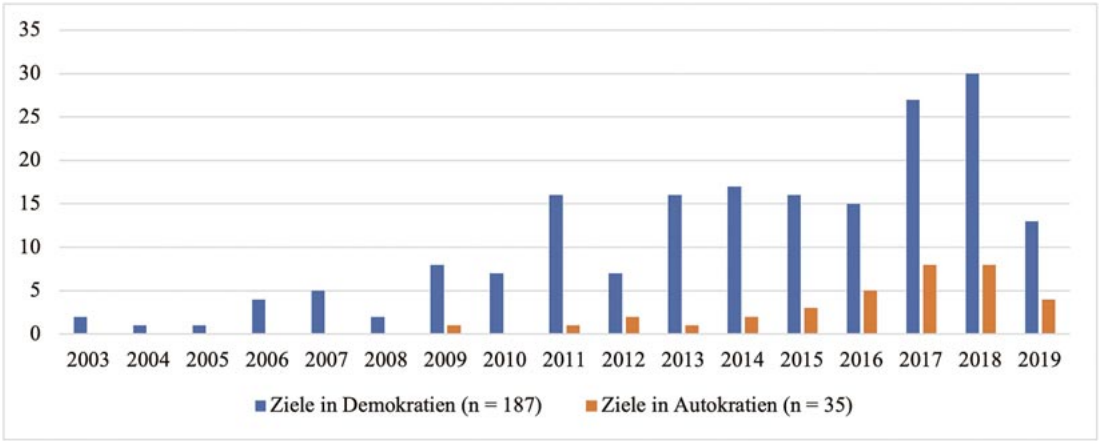

Abbildung 3: Autokratische Proxy-Operationen: Regimetyp der Ziele

zenposition ein. An zweiter Stelle rangiert die Russische Föderation, mit geringerem Abstand folgen auf Platz 3 und 4 der Iran sowie Nordkorea. Ein Befund, der sich mit dem bisherigen Forschungsstand zum autokratischen Cyberkonfliktaustrag weitgehend deckt (s. Schwartz 2017; Greenberg 2019a; Proofpoint 2017; Insikt Group 2019; Novetta 2016). Während wir hier einen Vergleich der chinesischen und russischen Operationen vornehmen, sind wir in dem 2022 veröffentlichten Sammelband (Zettl et al. 2022) in einer vergleichenden Studie den iranischen und nordkoreanischen Cyberproxy-Operationen nachgegangen (s. Abschnitt 7.1 sowie Zettl 2022a)

	Land	Fallanzahl
1	China	105
2	Russland	59
3	Iran	52
4	Nordkorea	33
5	Syrien	12
6	Vietnam	10
7	Vereinigte Arabische Emirate	5
8	Türkei	3

Tabelle 12: Autokratische Proxy-Operationen: Häufigkeit der attribuierten „Sponsors"

5.2 Vergleichende Fallstudie I: China vs. Russland

Im HD-CY.CON-Datensatz weisen die Volksrepublik China und die Russische Föderation nicht nur die höchste Anzahl von attribuierten Proxyoperationen auf. Sie rangieren auch in der Kategorie allgemein/direkt-staatlich attribuierter Cyberoperationen an der Spitze. Abbildung 4 weist zudem aus, dass eine gewisse Parallelität, bei geringer Fallzahl, zwischen den allgemein/direkt-staatlichen sowie staatlich-unterstützten Proxyoperationen beider Staaten zu bestehen scheint, da mit einem gewissen zeitlichen Versatz die jeweiligen Einsatzzahlen ansteigen bzw. fallen. Dabei ist die Anzahl der von beiden Staaten initiierten Operationen im Gesamtzeitraum deutlich angestiegen.[10]

Neben der bloßen Anzahl der jeweiligen Operationen sind hier vor allem die Operationsarten, i.e. Incident Types, von Interesse. Abbildung 5 zeigt dabei eine starke Prävalenz von Data Theft-Operationen mit und ohne Hijacking. Da viele Staaten auch im analogen Raum Spionage betreiben, ist dieser Befund nicht überraschend. Interessanter ist die Frage, ob sich durch regionale Schwerpunkte oder angegriffene Zielsysteme ein distinktes Verhaltensmuster erkennen lässt, bspw. entsprechend eines chinesischen Interesses an einer militärpolitischen Dominanz im Südchinesischen Meer oder dem Ausbau der Belt-Road-Initiative, oder Russlands militärischen Engagement in Staaten des Mittleren Ostens.

Neben der Gemeinsamkeit von Data Theft-Operationen weisen die chinesischen und russischen Cyberproxyoperationen aber auch eine interessante Varianz auf: Disruptive Operationsformen machen mit 15 Vorfällen für Russland

[10] Die Zahlen für die Operationsstartjahre 2018 & 2019 sind vorläufig und können sich durch zeitlich verzögerte Detektions- und Attributionsprozesse von neu bekanntwerdenden Vorfällen noch verändern.

rund 25,4 Prozent der verzeichneten Proxyoperationen aus. Zu diesen Operationen werden neben Disruption (mit oder ohne Hijacking) auch Doxing-Vorfälle gezählt, da der strategischen Veröffentlichung gestohlener Daten eine erhebliche Disruptionswirkung zukommen kann, i.e. die russische Einflussnahme auf den US-Präsidentschaftswahlkampf 2016 gezeigt hat (vgl. Whittaker 2019; Zettl 2019). Für die Volksrepublik China liegt der Anteil disruptiver Operationsformen unter 3 Prozent (3 von 105) und damit deutlich niedriger als für die Russische Föderation.

Datendiebstahl dominiert (bislang) das Operationsprofil der beiden untersuchten Staaten. Ob sich dieser Diebstahl aber gegen kommerzielle oder politische Ziele richtet, bspw. auf die transnationale Überwachung innerstaatlicher RegimegegnerInnen oder DissidentInnen abzielt, ist damit noch nicht geklärt. Unsere Daten zeigen (Abbildung 6), dass beide Autokratien ihre Operationen primär gegen politische/staatliche Institutionen und AkteurInnen richten, was aufgrund der Selbstzuschreibung als bedeutende Großmächte mit regionalen und globalen Interessen nicht weiter verwundern sollte. Es zeigen sich aber auch wichtige Unterschiede: Auf Rang 2 der von China anvisierten Ziele für Datendiebstahl finden sich private Unternehmen. In mehr als jedem dritten Fall dienen staatliche chinesische Cyberoperationen also ökonomischen Zie-

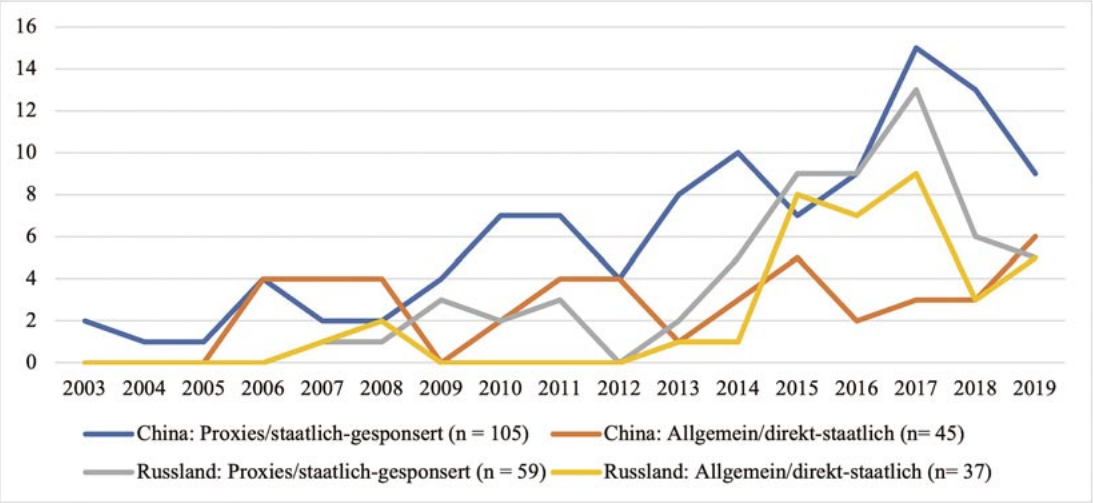

Abbildung 4: Verteilung der Operationsformen mit staatlicher Involvierung über Zeit

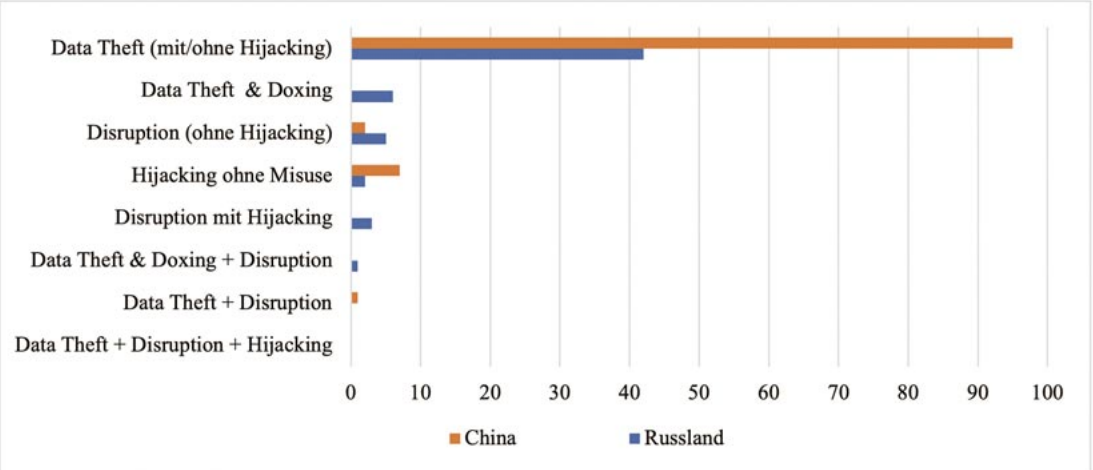

Abbildung 5: Incident Types chinesischer vs. russischer Cyberproxyoperationen

len. Der Diebstahl geistigen Eigentums zielt dabei offensichtlich auf das sogenannte „leapfrogging" Chinas im wirtschaftlichen Aufholwettkampf mit westlichen Industriestaaten ab, insbesondere den USA, um mit Hilfe von Wirtschaftsspionage ganze Entwicklungsstadien in strategischen Sektoren zu überspringen (vgl. Gilli und Gilli 2019). Angriffe auf kritische Infrastrukturen, auf Rang drei der chinesischen Cyberangriffsziele, entsprechen ebenfalls dieser wirtschaftlichen Zielsetzung, gerade im Gesundheits-, Chemie-, Verteidigungs-, sowie Transportsektor. Das Bild schärft sich, wenn man die Sequenz der durch chinesische AkteurInnen ausspionierten Wirtschaftssektoren betrachtet: So lässt sich ein deutlicher Zusammenhang zwischen den attackierten Sektoren und den wirtschaftlichen Zielsetzungen der jeweiligen Fünf-Jahres-Pläne der KPC erkennen (vgl. Chon und Clover 2015; Welgan 2017; Sabbagh 2021).

Russische Cyberoperationen attackieren deutlich seltener private Unternehmen als chinesische. Russische Angriffe richten sich vielmehr neben politischen/staatlichen Zielen ähnlich stark auf kritische Infrastrukturen wie auf zivilgesellschaftliche AkteurInnen und Einrichtungen, i.e. wissenschaftliche und Bildungseinrichtungen sowie Medienorganisationen und einzelne JournalistInnen.

Ein spezifischerer Blick auf die im HD-CY.CON verzeichneten Subtypen politischer und staatlicher Ziele verdeutlicht die besondere Relevanz des Diebstahls sensibler Informationen von ausländischen Regierungs- und Ministerialinstitutionen. Unter den politischen Zielen rangieren sie für beide Länder an erster Stelle (Abbildung 7). Es folgen jeweils militärische Ziele auf dem zweiten Rang: Im russischen Fall weist dies auf die stetig gestiegene Bedeutung von Cyberspionage und disruptivere Operationsformen im Kontext des Ukrainekrieges hin (ab 2014) (Maurer und Geers 2015; Perez 2016; Tucker 2018; Maschmeyer 2021). Für China stehen (bislang) militärpolitische Ziele im Kontext des Konflikts um das Südchinesische Meer im Vordergrund (Proofpoint 2017), aber auch US-Militäreinrichtungen werden im Rahmen der strategischen Rivalität beider Länder um die Führungsposition in politischen, militärischen sowie wirtschaftlichen Sektoren attackiert (vgl. Goldstein 2015; Zhao 2021).

Russische Cyberproxyoperationen dienen zudem immer häufiger der Unterwanderung demokratischer Willensbildungs- und Wahlprozesse, wie etwa 2016 in den USA (Calabresi 2017; Hansen und Lim 2019; Zettl 2019) oder in vielen

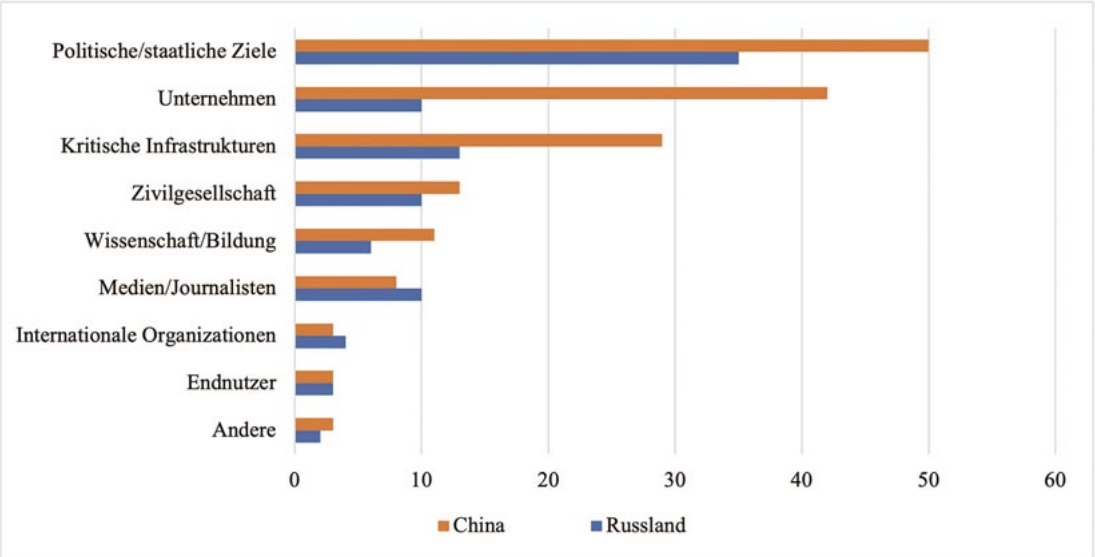

Abbildung 6: Ziele chinesischer und russischer Cyberproxyoperationen

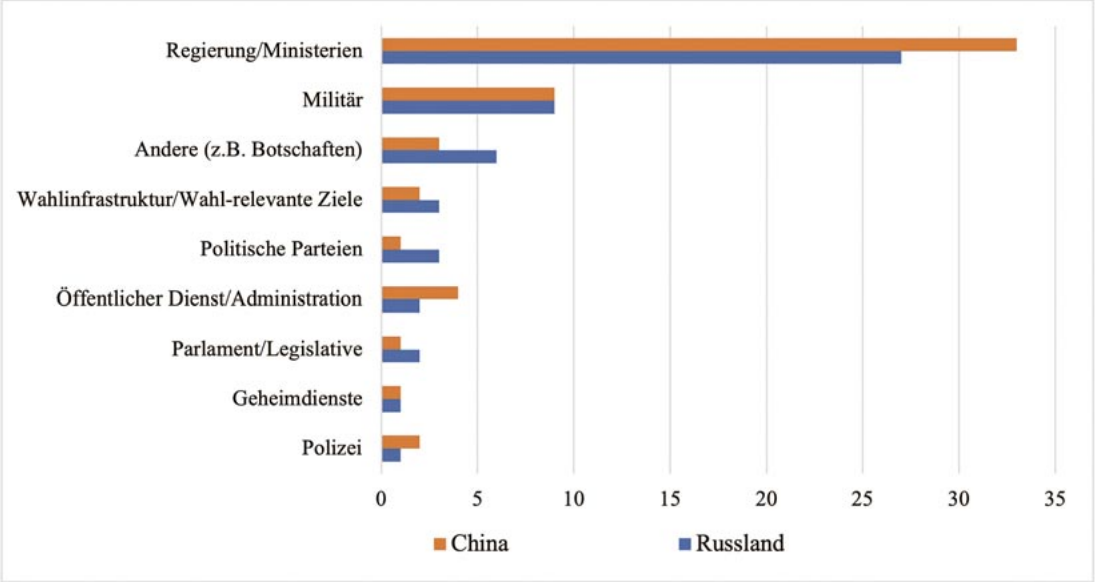

Abbildung 7: Subtypen politischer/staatlicher Ziele chinesischer vs. russischer Cyberproxy-operationen (Gesamtzeitraum)

osteuropäischen Staaten, wie der Ukraine oder dem Baltikum (Sytas 2019; Backes und Swab 2019). Ein ähnliches Operationsprofil lässt sich mittlerweile auch für chinesische Angriffe auf Ziele in Taiwan und Hongkong feststellen (Manantan 2020).

Analysiert man den Modus Operandi chinesischer Cyberproxyoperationen im Rahmen konventioneller Konflikte, z. B. im Südchinesischen Meer, so fällt auf, dass es (bislang) nur wenige disruptive Attacken und dafür in der Mehrzahl Spionageakte gab. Im Vergleich sind russische Cyberproxyoperationen deutlich disruptiver: am bekanntesten sind die beiden Stromausfälle (2015 & 2016) in der Ukraine, die durch Cyberangriffe der russischen Gruppierung Sandworm verursacht wurden (Greenberg 2019b).

Abbildung 8 verdeutlicht in diesem Kontext, dass chinesische Proxyoperationen häufig im Zusammenhang mit (gewaltlosen und auch gewalttätigen) Offline-Konflikten stehen. In Relation ist der Anteil russischer Cyberproxyoperationen zwar zahlenmäßig deutlich geringer, in gewaltsamen Offline-Konflikten ist dieser aber höher als bei nicht-gewaltsamen Konflikten, was auf ein robusteres Einsatzprofil für russische Cyberproxies hindeutet.

Im Detail waren chinesische Proxyoperationen in gewaltsamen Offline-Konflikten primär auf strategische Spionageoperationen gerichtet. Die in Abbildung 5 verzeichneten sieben Vorfälle von Hijacking ohne direkt erkennbarem Misuse chinesischer Proxies könnten aber auch darauf hindeuten, dass diese Infiltrationen für künftige Sabotageakte in den Zielnetzwerken genutzt werden sollen, bspw. wenn es die Zuspitzung der Konfliktsituation aus chinesischer Sicht erforderlich macht.[11] Entsprechende Hinweise auf disruptivere Cyberoperationen chinesischer Hacker gab es zuletzt im Rahmen der gewaltsamen Auseinandersetzungen mit Indien im Himalaya-Gebirge (Joshi 2020).

Fasst man diese Befunde zusammen, so ergibt sich folgendes Bild: Chinesische Cyberspionageoperationen dienen bislang primär der wirtschaftlichen Entwicklung des Landes, insbeson-

[11] Durch das Errichten von „beachheads" in fremden Systemen können sog. „logic bombs" platziert und zu einem späteren Zeitpunkt aktiviert werden, um die intendierte Schadwirkung zu entfalten (Klimburg 2011, S. 42).

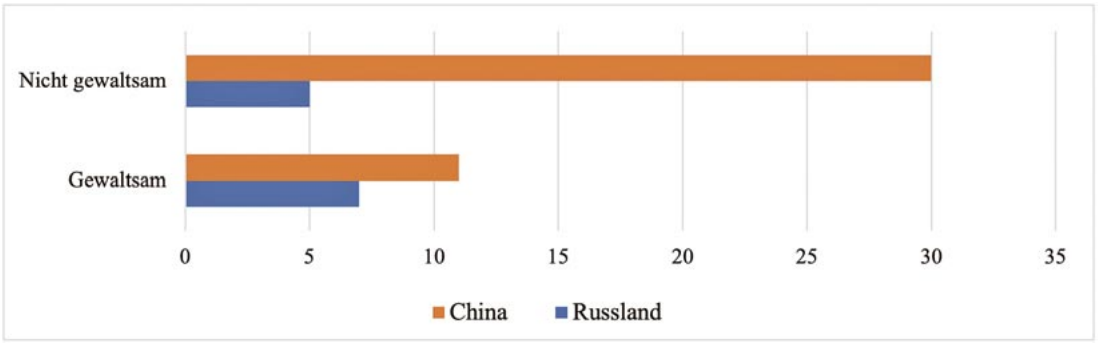

Abbildung 8: Kodierte Offline-Konflikte für russische & chinesische Proxy-Operationen (Gesamteitraum)

dere dem (nachträglichen) technologischen Übertreffen westlicher Industriestaaten in strategischen Sektoren und lediglich sekundär der Flankierung militärischer Operationen in territorialen Konflikten (Südchinesisches Meer, Doklam). Russische Cyberproxyangriffe sind im Untersuchungszeitraum zwar seltener als chinesische, dafür jedoch disruptiver, insbesondere wenn sie auf die Schwächung des Gegners in konventionellen Konflikten gerichtet sind. Russische Operationen mit politischen Zielen dienen der Spionage, bspw. in internationalen Organisationen (s. Stewart 2009), aber vor allem auch der Unterwanderung des demokratischen Willensbildungs- und Wahlprozesses in ausgewählten westlichen Zielstaaten.

Bevor wir auf die Entwicklung des Proxygebrauchs durch demokratische Regierungen eingehen, widmen wir uns den Akteurscharakteristika der eingesetzten Proxygruppen als auch den unterschiedlichen Modi staatlicher Kontrolle. In Tabelle 13 finden sich die im HD-CY.CON verzeichneten chinesischen Proxygruppen gelistet, die der chinesischen Volksbefreiungsarmee (PLA) oder dem chinesischen Ministerium für Staatssicherheit (MSS) als verantwortlicher staatlicher Stelle zugeordnet werden. Die Benennung der Gruppierungen folgt dabei der gebräuchlichen Namensgebung durch private IT-Unternehmen in der kommerziellen Threat Intelligence Research.[12]

Unsere Untersuchung zeigt deutlich, dass der Einsatz von PLA- und MSS-Proxies über Zeit variiert: So wurden unter Präsident Hu Jintao (2003 bis 2012) jeweils zehn Proxyoperationen der PLA sowie dem MSS zugesprochen.[13] Inhaltlich waren dabei beide Akteursgruppen in der Wirtschaftsspionage involviert, bspw. der PLA-Proxy APT1. Dass auch militärisch-assoziierte HackerInnen in dieser Periode Wirtschaftsspionage betrieben, kann zunächst als Hinweis auf eine wenig ausdifferenzierte Arbeitsteilung angesehen werden. Wahrscheinlicher jedoch ist, dass die Militarisierung der Wirtschaftsspionage auf eine Verschränkung zwischen Wirtschaftsspionage und militärischer Modernisierung, wie im Fall der Spionage der Konstruktionspläne des F-35 Jets im Jahr 2007, hindeutet (Gady 2015).

In der bisherigen Amtszeit Xi Jinpings (2013-2019) wurden nur zehn PLA-Proxyoperationen aber 26 MSS-Proxyoperationen im HD-CY.CON verzeichnet. Diese Akzentverschiebung in der Kontrollstruktur der CyberstellvertreterInnen korrespondiert mit der im Jahr 2015 begonnenen Umstrukturierung der Zuständigkeiten innerhalb der chinesischen Sicherheitsarchitektur. So wurde die Rolle des MSS im Cyberraum ge-

[12] In Klammern befinden sich weitere Informationen zu der jeweilig verantwortlichen PLA- oder MSS-Einheit, sowie im Falle von APT3/Gothic Panda dem als MSS-Proxy fungierenden Technologie-unternehmen Boyusec.

[13] Diese sowie die nachfolgenden Zahlen beziehen sich auf die 105 als chinesische Proxoperationen attribuierten Incidents, plus zehn weitere allgemein/direkt-staatlich attribuierte Fälle mit chinesischer Verantwortung von PLA- sowie MSS-Gruppierungen (APT1/Comment Crew, APT30/Naikon, APT10/Stone Panda), die im Datensatz über Zeit sowohl mit einer 1 als auch einer 2 (bzw. 2,1) im Rahmen der Initiator Category bewertet wurden und somit ebenfalls zumindest als zeitweilige Proxies angesehen werden.

stärkt und die Mehrzahl der attribuierten Spionageoperationen dem MSS zugeschrieben. Die 2015 etablierte Strategic Support Force der PLA fokussierte sich stärker auf den Ausbau offensiver Cyberoperationsfähigkeiten mit disruptiver Wirkung im Rahmen konventioneller Offline-Konflikte.

Neben der militärischen Modernisierung der PLA wurde auch der Druck der Obama-Administration für die Akzentverschiebung in der Kontrolle chinesischer Cyberproxies verantwortlich gemacht. Entsprechende US-Sanktionsdrohungen führten 2015 zur Unterzeichnung des Obama-Xi-Agreements, welches beide Regierungen dazu verpflichtete, keine Wirtschaftsspionage im Cyberraum zu betreiben (Rollins 2015). In der unmittelbaren Folge verzeichneten IT-Sicherheitsunternehmen einen signifikanten Rückgang chinesischer Spionageoperationen auf US-Ziele. Ab dem Jahr 2017 setzten die Spionageoperationen durch Proxies des MSS wieder ein, die sich nach Angaben des US-Justizministeriums oftmals aus Angehörigen privater IT-Unternehmen rekrutieren (s. DoJ 2017b; DoJ 2021). Unter Präsident Trump kam es zu einer deutlichen Verschlechterung der bilateralen Beziehungen, insbesondere in der Handelspolitik, sodass zusätzliche Anreize für eine Wiederaufnahme der Spionageaktivitäten geschaffen wurden.

People´s Liberation Army (PLA)	Ministry of State Security (MSS)
APT1/Comment Crew/Byzantine Candor (Unit 61398)	Winnti Group (Xicheng District, Peking)
APT30/Naikon (Unit 78020)	APT3/Gothic Panda (Boyusec)
Tick (Unit 61419)	APT10/Cloud Hopper (Tianjin State Security Bureau)
Red Foxtrot (Unit 69010)	APT17/Deputy Dog (Jinan Bureau)
Tonto Team/Cactus Pete (Unit 65017)	APT26/Turbine Panda (Jiangsu Bureau)
APT19/Deep Panda/Black Vine (Unit unbekannt)	APT40/Temp.Periscope (Hainan State Security Department/Hainan Xiandu)
	APT41/Leviathan (Chengdu 404 Network Technology)

Tabelle 13: Institutionelle Affiliationen der im HD-CY.CON erfassten chinesischen Proxies[14]

FSB (Ziviler Inlandsgeheimdienst)	GRU (Militärgeheimdienst)	SVR (Ziviler Auslandsgeheimdienst)
Turla/Snake/Uroburos	Fancy Bear/APT28 (Unit 26165)	Cozy Bear/APT29
Gamaredon	Sandworm Team/Voodoo Bear (Unit 74455)	

Tabelle 14: Institutionelle Affiliationen der im HD-CY.CON erfassten russischen Proxies

[14] Diese Tabelle erfasst ausschließlich jene chinesischen APTs im HD-CY.CON, denen bislang öffentlich eine PLA- oder MSS-Affiliation zugesprochen wurde. Es existieren daneben noch weitere chinesische Proxy-Gruppierungen, die vom HD-CY.CON erfasst werden, z.B. APT27/Emissary Panda, APT15/Mirage, APT20, APT31/Zirconium usw. Weitere chinesische Proxy-Gruppierungen sind im HD-CY.CON vorgemerkt aber noch nicht erfasst worden, wie etwa die für den Microsoft-Exchange-Hack verantwortlich gemachte HAFNIUM-Gruppierung oder auch die von Recorded Future 2020 identifizierte Gruppe TAG-22 (Microsoft Threat Intelligence Center 2021; Insikt Group 2021), deren Operationen in den Startjahren 2020 bzw. 2021 stattfanden.

Vergleicht man die chinesische Kontrollstruktur für Cyberproxies mit jener russischer CyberstellvertreterInnen, so ist auffallend, dass sich eine große Anzahl chinesischer Proxygruppierungen (insgesamt 35-37 im HD-CY.CON)[15] für ähnlich viele Angriffe verantwortlich zeichnete. In Russland wurden indes 67 der 96 erfassten Cyberoperationen mit attribuierter Involvierung des russischen Staates (Initiator Categories 1, 2 und 2,1) allein von vier Gruppierungen/APTs durchgeführt: Fancy Bear aka APT28, Cozy Bear aka APT29, Sandworm aka Voodoo Bear sowie Turla aka Snake/Waterbug. Hinzu kommen sechs Operationen der Gruppierungen Gamaredon Group und Energetic Bear aka Dragonfly. Tabelle 14 veranschaulicht die zugeschriebenen Verbindungen zwischen Proxygruppen und militärischen und zivilen Geheimdiensten in Russland (GRU; FSB & SVR).

Das Operationsprofil der beiden GRU-Gruppierungen Fancy Bear & Sandworm, die seit 2017 in öffentlichen Zuschreibungen immer stärker als aktive GRU-Einheiten und weniger als Proxies ausgewiesen werden, entspricht im Rahmen des Ukrainekonflikts dem Profil eines militärischen Geheimdiensts. Gleiches gilt auch für die im November 2021 durch den ukrainischen Security Service identifizierte Gamaredon Group mit FSB-Affiliation (aka Armagedon Group; SSU 2021), die ebenfalls im Kontext der militärischen Auseinandersetzungen in der Ostukraine Cyberoperationen verübte (Tucker 2018).

Russischen Geheimdiensten wurde im Cyberraum zudem ebenso wie im analogen Raum ein Hang zu bürokratischen Machtkämpfen („Turf-War") nachgesagt (Galeotti 2015 & 2016). So kam es Anfang 2019 zu einem Skandal um FSB-Offiziere, die dem FBI geheime Informationen u.a. über die Involvierung des GRU in die US-Wahlbeeinflussung 2016 geliefert haben sollen. Diese Kompromittierung wurde durch den GRU aufgedeckt und die entsprechenden FSB-Mitglieder vor Gericht gestellt (Eckel 2019).

Ein weiteres Merkmal russischer Cyberproxy-Nutzung ist der Einsatz inländischer oder im Ausland ansässiger, russisch-stämmiger Cyberkrimineller, die ähnlich wie die verstärkte Nutzung privater Technologieunternehmen durch das chinesische MSS, eine Alternative zu den bisherigen Proxygruppen bilden. So sollen staatliche Stellen russische Cyberkriminelle zu Ransomware-Operationen im April 2021 angestiftet haben, ein Auftragsmuster, das bereits in den sog. „Yahoo-Hacks" (2013 & 2014) praktiziert wurde. In diesem Falle hatten FSB-Offiziere zwei Cyberkriminelle direkt mit den Hacks beauftragt und ihnen die notwendigen technischen Tools bereitgestellt, wie die Anklageschrift des US-Justizministeriums feststellte (DoJ 2017a).

Abschließend lässt sich konstatieren, dass die Konfidenz der Zuschreibung von chinesischen und russischen Cyberproxybeteiligungen durch politische oder privatwirtschaftliche AkteurInnen erheblich variiert. Chinesische Cyberproxyinvolvierungen werden regelmäßig mit hoher Konfidenz und von mehreren AkteurInnen zugeschrieben, während die Attribution für russische CyberstellvertreterInnen ambivalenter ausfällt. So wurden für die vier Hauptgruppen nicht nur zahlreiche Proxybeziehungen zugeschrieben, sondern auch allgemein/direktstaatliche Attributionen vorgenommen, ohne dass eine klare zeitliche Zuordnung bspw. durch unterschiedliche IT-Sicherheitsunternehmen erkennbar wäre.

[15] Aufgrund überlappender Namensgebungen seitens IT-Unternehmen lässt sich die exakte Anzahl tatsächlich distinkter Gruppierungen nur schwer festlegen.

5.3 Demokratische Cyberproxies im HD-CY.CON: Eine Übersicht

Regierungen demokratischer Staaten nutzen andere Cyberproxies für andere Zwecke als autokratische Regierungen, so unsere Ausgangsvermutung. In unserem liberalen Erklärungsmodell sollten demokratische Regierungen versuchen in asymmetrischen Interdependenzbeziehungen die relativ größere Verwundbarkeit ihrer offenen Gesellschaften, die aus einem relativ höheren Digitalisierungsgrad der Gesellschaft und einem unbeschränkteren Zugang von Computernetzwerken resultiert, dadurch zu kompensieren, dass nicht alle Cyberangriffe öffentlich attribuiert werden. So kann der in Demokratien (höhere) öffentliche Druck auf eine Angriffserwiderung und die damit verbundene Eskalation vermieden werden, insbesondere, weil die bestehende Verwundbarkeitsasymmetrie eine weitere Eskalation verlustträchtig erscheinen lässt. In einer solchen Informationsasymmetrie nutzen demokratische Regierungen, aber nicht nur diese, die technische Attribution durch IT-Sicherheitsfirmen, sodass die TäterInnen zwar informiert werden, dass ihr Angriff detektiert wurde, aber die Angreifenden im Ungewissen darüber gelassen werden, welche politischen rechtlichen Folgen der Angriff (noch) zeitigen wird.

Abbildung 9 veranschaulicht zunächst die zentralen Befunde des HD-CY.CON zur zeitlichen Entwicklung von Cyberangriffsattributionen, die eine staatliche Involvierung auf der AngreiferInnenseite beinhalteten (allgemein/direktstaatliche Attributionen oder staatlich-gesponserte Proxyoperationen). Im Laufe der zwei erfassten Jahrzehnte nahm dabei die Anzahl der Attributionen insgesamt stetig und deutlich zu, der vorläufige Höhepunkt wurde im Jahr 2018 erreicht. Zwei Einschränkungen sollten aber bedacht werden: Zum einen ist die Untersuchung der Zahlen für die Attributionsjahre 2020 und 2021 noch nicht vollständig abgeschlossen; zum anderen sagt die Anzahl der Angriffe noch nichts über deren Ziele und Kosten aus. Insgesamt verdeutlicht die Abbildung jedoch, dass nicht nur die offensiven Cyberoperationen im Laufe des Untersuchungszeitraums stetig zugenommen, sondern auch, dass die attribuierenden AkteurInnen diese immer häufiger staatlichen UrheberInnen öffentlich zugeschrieben haben.

Abbildung 10 zeigt, welche AkteurInnen die Attributionen von staatlichen oder staatlich-gestützten Proxyangriffen vornahmen. Auffällig ist, dass auf dem ersten Platz mit großem Abstand IT-Unternehmen aus demokratischen Ländern rangieren, mit 199 erfassten Attributio-

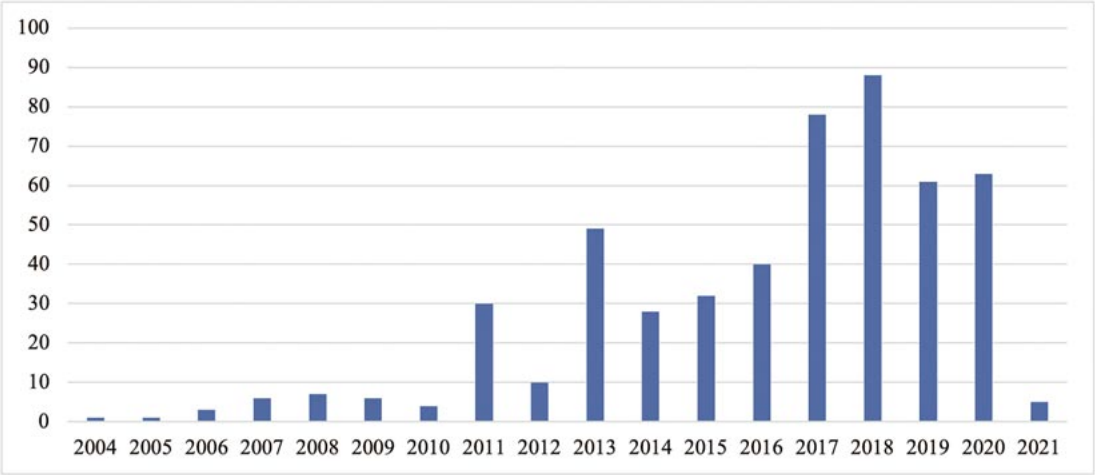

Abbildung 9: Cyberoperationen, die staatlichen AngreiferInnen oder Proxies zugeschrieben wurden, geordnet nach dem Jahr der Attribution

nen der beiden AngreiferInnenkategorien. Im Vergleich verzeichnet der HD-CY.CON mit 89 Vorfällen deutlich weniger Attributionen politischer/staatlicher AkteurInnen aus Demokratien. Eine liberale Interpretation lässt auf zweierlei schließen: Einerseits sollten private IT-Unternehmen einen kommerziellen Anreiz haben, möglichst viele Cyberangriffe technisch zu attribuieren, denn sie profitieren unmittelbar von der zusätzlichen Transparenz, sofern sie IT-Sicherheitsdienstleistungen anbieten, indem Schutzmaßnahmen nach berichteten Angriffen häufiger nachgefragt werden. Andererseits kann die relative Zurückhaltung bei der Attribution demokratischer Regierungen darauf zurückgeführt werden, dass die Regierungen die Eskalationskontrolle gegenüber einer kritischen demokratischen Öffentlichkeit bewahren möchten und/oder Informationsasymmetrien gegenüber den Angreifenden – Zeit für Detektions- und Erwiderungsmaßnahmen – nutzen möchten (Carnegie 2021, S. 217).

Berichtenswert ist ferner, dass demokratische IT-Unternehmen, und mit Abstand auch demokratische Regierungen, deutlich häufiger Cyberoperationen mit vermuteter, staatlicher Beteiligung attribuieren als ihre autokratischen Pendants. Für die 46 verzeichneten Attributionen von IT-Sicherheitsfirmen aus autokratischen Staaten waren überwiegend zwei Unternehmen verantwortlich: das auch international (sehr) erfolgreiche Unternehmen Kaspersky aus Russland sowie Attributionen des aufstrebenden chinesischen Technik-Sektorunternehmens Qihoo 360.

Cyberoperationen, in denen IT-Unternehmen und politische/staatliche AkteurInnen aus Demokratien attribuieren sind selten(er). Der HD-CY.CON verzeichnet lediglich 32 Vorfälle mit doppelter Attribution. In diesen Fällen ersetzen technische Attributionen politische Verantwortungszuweisungen nicht vollständig. Vielmehr dürften vorgängige politische Attributionen gestärkt werden, wenn spezifische technische Evidenzen die Legitimität der politischen Zuschreibung erhärten.

Wenn wir auf die Herkunftsländer jener IT-Sicherheitsunternehmen blicken, die am häufigsten Cyberoperationen zuschreiben, dann ergibt sich

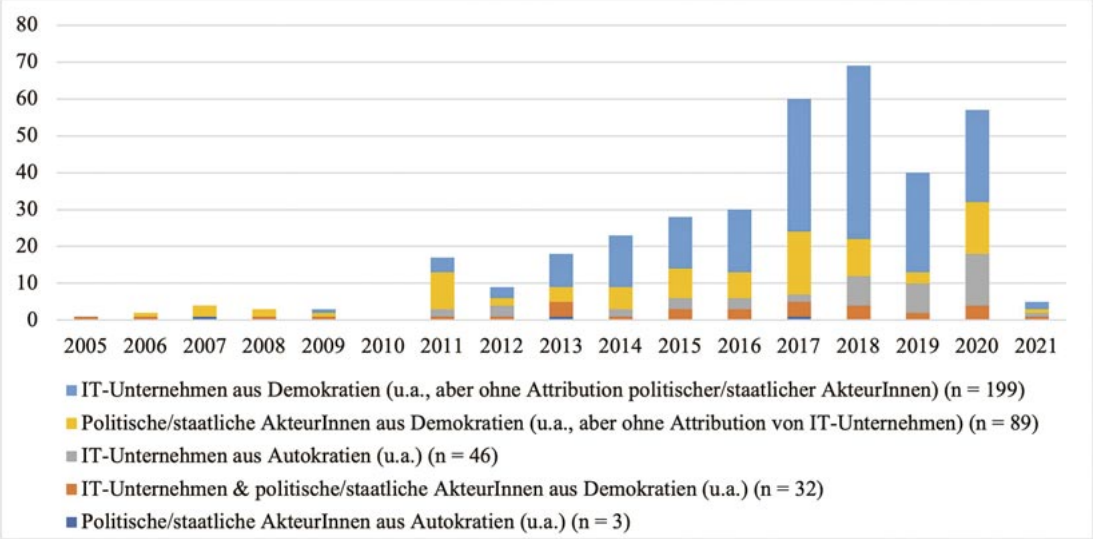

Abbildung 10: Die Attributionsquellen von Cyberoperationen mit staatlicher Involvierung auf der AngreiferInnenseite (allgemein/direkt-staatliche AngreiferInnen oder Proxies)

Anmerkung: Die Zahlen beziehen sich auf einzelne und kombinierte Attributionsquellen für Fälle, in denen diese jeweils eine staatliche Involvierung auf der AngreiferInnenseite attribuiert haben, das Initiator Country kann dabei jedoch unbenannt geblieben sein.

folgendes Bild (Tabelle 16): Die USA führen die Rangliste mit 217 weit vor allen anderen Staaten an. Dies weist sicherlich auf die Stärke US-amerikanischer Unternehmen im IT-Sektor und die Bedarfe hin, die sie abdecken; es kann aber auch als Ausdruck der technischen Dominanz der US-basierten Dateninfrastruktur für das gesamte Internet betrachtet werden, die es IT-Sicherheitsfirmen als auch US-Regierungsinstitutionen erlaubt, einen erheblichen Teil der weltweiten Datenströme zu erfassen bzw. zu überwachen.

Auf dem zweiten Platz folgen IT-Unternehmen aus Russland, die 49 Attributionen vornahmen, hauptsächlich Kaspersky. Israelische IT-Unternehmen waren für 31 Attributionen verantwortlich und damit deutlich mehr als im viertplatzierten Staate, der Slowakei, indem ein Unternehmen, ESET, für alle 15 Zuschreibungen verantwortlich zeichnete. Eine ähnlich dominante Stellung nehmen die IT-Sicherheitsfirmen TrendMicro in Japan, Bitdefender in Rumänien, sowie F-Secure in Finnland ein.

Im Vergleich zu den USA aber auch Asien weist Tabelle 15 auch auf die relative Attributionsschwäche der IT-Community in der Europäischen Union hin, die insgesamt wenige, in den

	Land	Attributionsanzahl*	Regimetyp
1	USA	217	Demokratie
2	Russland	49	Autokratie
3	Israel	31	Demokratie
4	Slowakei	15	Demokratie
5	Japan	10	Demokratie
6	China	8	Autokratie
7	Großbritannien	6	Demokratie
8	Niederlande	5	Demokratie
9	Rumänien	5	Demokratie
10	Finnland	4	Demokratie
11	Spanien	2	Demokratie
12	Taiwan	2	Demokratie
13	Kuwait	2	Autokratie
14	Deutschland	2	Demokratie
15	Indien	1	Demokratie
16	Italien	1	Demokratie
17	Kanada	1	Demokratie
18	Tschechien	1	Demokratie
19	Südkorea	1	Demokratie
20	Iran	1	Autokratie

Tabelle 15: Die Herkunftsländer attribuierender IT-Unternehmen im HD-CY.CON

Anmerkung: Gelistet sind hier nur Attributionen mit mindestens einer positiven Kodierung der Initiator Category oder Initiator Country Kategorie (oder beidem). Diese Tabelle enthält somit sowohl „True", als auch „Blurred Attributions", nicht aber technische Berichte, in denen keine der beiden AngreiferInnen-Kategorien durch das IT-Unternehmen attribuiert wurden. In manchen Fällen attribuierten mehrere IT-Unternehmen aus unterschiedlichen Ländern dieselbe Operation.

Staaten Osteuropas aber deutlich stärkere Aktivitäten im Untersuchungszeitraum entfaltete als in Mittel- und Westeuropa.

Insgesamt ergibt sich aus der Betrachtung der Häufigkeitsverteilung der demokratischen Attributionsvorgänge, dass die USA und Israel als plausible Untersuchungsstaaten für den Demokratievergleich gelten können. Zum einen lässt sich dies mit dem vergleichsweise starken Attributionsengagement der jeweiligen IT-Sektoren begründen; zum anderen gehen die jeweiligen Attributionen von mehreren Unternehmen aus. Darüber hinaus sind beide Staaten in diverse Regionalkonflikte im Nahen Osten (USA & Israel), als auch Europa (USA) involviert, sodass potenzielle Varianzen in der Nutzung von defensiven Cyberproxies in gewaltsamen vs. gewaltlosen Offlinekonflikten zu interessanten Erkenntnissen führen könnten.

5.4. Vergleichende Fallstudie II: USA vs. Israel

Die USA und Israel verfügen über stark entwickelte und weltweit führende Technologie-Unternehmen. So wird Israel zuweilen sogar als „Start-Up-Nation" bezeichnet (Behar 2016). Der HD.CY-CON zeigt deutlich, dass diese Firmen auch im Bereich der Threat Research Intelligence und Attribution eine weltweit dominante Stellung einnehmen. US-Sicherheitsunternehmen wiesen in 178 Fällen staatlichen AkteurInnen oder ihren Proxies die Verantwortung für Cyberoperationen zu. Israelische Firmen attribuierten 24 derartige Angriffe. Bislang weisen die analysierten Operationen das Jahr 2018 als Höhepunkt aus, die Auswertung der Folgejahre ist indes nicht abgeschlossen.

In Abbildung 11 wurden auch Attributionsfälle ausgewiesen, in denen zwar die AngreiferInnenkategorie, nicht aber das Herkunftsland benannt wurde, sog. „blurred attributions". Abbildung 12 gibt nun Aufschluss über jene Fälle, in denen durch amerikanische und israelische IT-Unternehmen sowohl die staatliche Institution oder der Proxy als auch das Herkunftsland in einer Zuschreibung genannt wurden, i.e. „true attributions". Der Anteil der „true attributions" überwiegt eindeutig jene Fälle, in denen technische Berichte zwar einen Angriff benennen, i.e. detection", aber weder die AngreiferInnenkategorie noch deren Herkunftsland identifizieren. Kurz: Wenn IT-Unternehmen in diesen Staaten attribuieren, dann wird mit hoher Wahrschein-

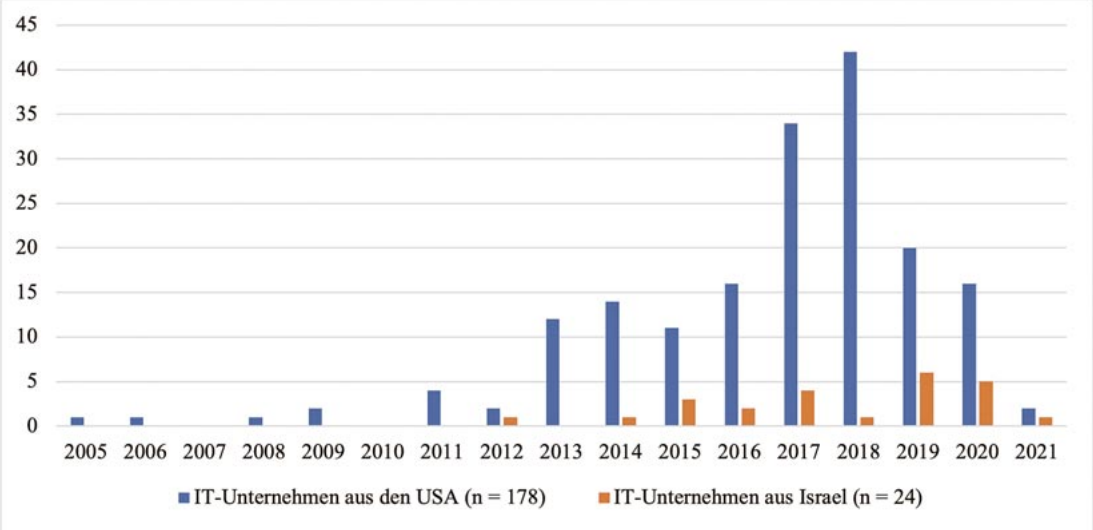

Abbildung 11: IT-Unternehmen als Attributionsquelle, Jahr der Attribution, staatliche Involvierung attribuiert

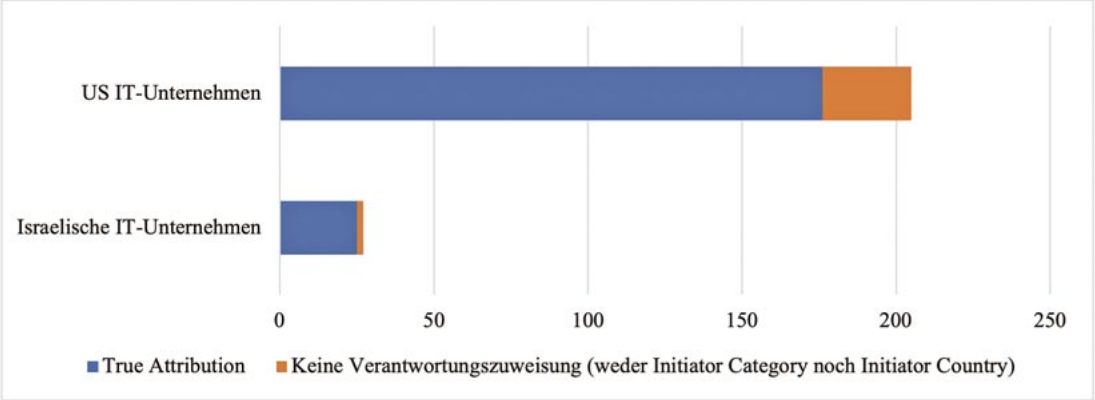

Abbildung 12: „True Attributions" amerikanischer und israelischer IT-Unternehmen

Anmerkung: Diese „True Attributions" beziehen sich ausschließlich auf Fälle, in denen eine staatliche Verantwortlichkeit auf der AngreiferInnenseite attribuiert wurde.

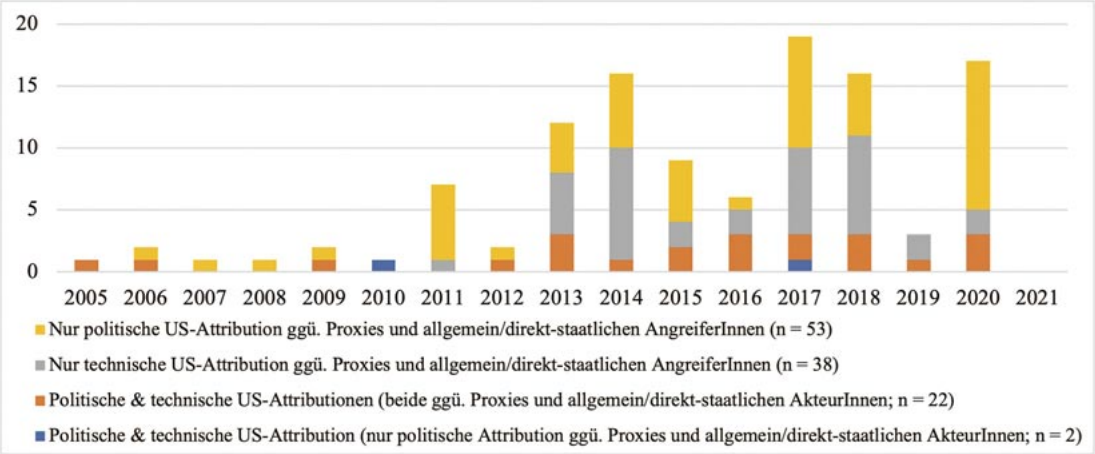

Abbildung 13: Fälle mit sowohl politischen, als auch technischen Attributionen von US-AkteurInnen für Operationen mit US-Zielen

Anmerkung: Die Zahlen beziehen sich auf einzelne und kombinierte US-Attributionsquellen für Operationen mit US-Zielen, in denen diese Quellen eine staatliche Involvierung auf der AngreiferInnenseite attribuiert haben, das Initiator Country kann dabei jedoch unbenannt geblieben sein.

lichkeit auch der (vermutete) Angreifer benannt, sodass die jeweilige Gruppe/Institution als „Tatverdächtiger" identifiziert und damit „gewarnt" ist.

Wie verhält sich die technische zur politischen Attributionspraxis in beiden Staaten? Unsere Datensammlung zeigt für die USA (Abbildung 13), in welchen Operationen mit US-Zielen ausschließlich politische oder technische Attributionen gegenüber staatlichen AkteurInnen vorgenommen wurden und wann politische AkteurInnen und nationale IT-Unternehmen attribuierten und in welchen Fällen einer doppelten Attribution lediglich die politische Attribution eine staatliche Verantwortlichkeit unterstellte.[16]

[16] Der umgekehrte Fall, dass im Falle einer doppelten Attribution nur das jeweilige IT-Unternehmen eine staatliche Involvierung auf der AngreiferInnenseite attribuierte, wurde im Datensatz nicht festgestellt.

Die hohe Zahl von ausschließlich politischen Attributionen (53) gegenüber staatlichen AngreiferInnen lässt darauf schließen, dass politische US-AkteurInnen primär „true attributions" vornehmen. Setzt man diese hohe Zahl ins Verhältnis zum deutlich geringeren Anteil technischer US-Attributionen mit staatlicher Verantwortlichkeit im Jahr 2020, so lässt sich für diesen Zeitabschnitt keine generelle Attributionszurückhaltung durch US-Regierungsinstitutionen nachweisen. Nach einem zeitweisen Rückgang der Attributionen im Jahr 2016 stieg der Anteil ausschließlich politischer US-Attributionen zudem im Jahr 2020 nochmal deutlich an, was u.a. auf die wachsende Anzahl von attribuierten Cyberspionage-Operationen im Zuge der Corona-Pandemie zurückgeführt werden kann (vgl. Bing und Taylor 2020).

Die Daten in Abbildung 13 legen auch nahe, dass im Fall einer doppelten Attribution (technisch und politisch), sich deren Verantwortungszuweisungen bislang nur selten signifikant voneinander unterschieden haben (zweimal).

Interessanterweise verzeichnet der HD-CY.CON-Datensatz für israelische Unternehmen keine Verantwortungszuweisungen für Fälle mit israelischen Zielen, in welchen ebenfalls Regierungsinstitutionen eine staatliche Involvierung auf der AngreiferInnenseite attribuiert haben (Abbildung 14). Operationen gegen israelische Ziele wurden in fünf Fällen ausschließlich technisch attribuiert, in zwei Fällen ausschließlich politisch. Dieser Befund kann auf die geringe Anzahl der beobachteten Fälle zurückgehen, insbesondere, wenn man diese mit der hohen Anzahl der US-Attributionen vergleicht. Die Daten in Abbildung 14 lassen aber auch folgende Interpretation zu: Regierungsinstitutionen in Israel üben (bislang) und insbesondere im Vergleich zu den US-Behörden eine stärkere Attributionszurückhaltung aus, während israelische IT-Unternehmen zumindest in einzelnen Fällen die Verantwortungszuweisung übernommen haben könnten. Da die israelische Regierung auch in anderen sicherheitspolitischen Fragen Geheimhaltung nutzt, um Israels Kontrahenten im Ungewissen über dessen Fähigkeiten (Nuklearwaffen) oder Einsatzrichtlinien (konventionelle Präemption gegen nukleare Standorte) zu belassen, fügt sich die zurückhaltende staatliche Attribution in ein etabliertes Politikmuster ein (Cohen 2010): Anstatt durch die Preisgabe von geheimdienstlichen Erkenntniswegen der Detektion von Cyberangriffen dem Gegner zu signalisieren, dass dessen Bemühungen (auch in Zukunft) erfolglos bleiben werden, sendet die israelische Regierung kein öffentliches Signal, sondern lässt den Angreifenden im Dunkeln über den Kenntnisstand und das weitere Vorge-

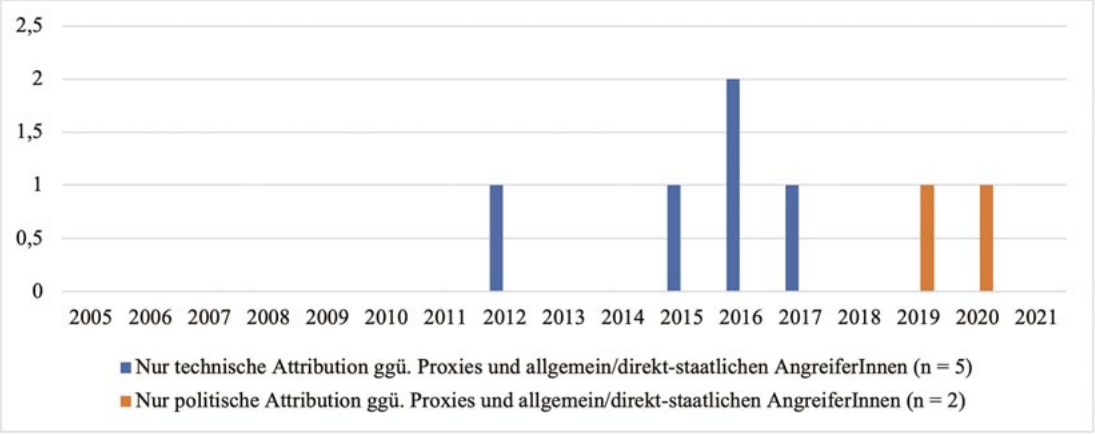

Abbildung 14: Israelische Attributionen für Fälle mit israelischen Zielen im Vergleich

Anmerkung: Das Initiator Country kann bei den hier erfassten Attributionen unbenannt geblieben sein.

hen der israelischen Regierung. Ein Grund hierfür könnte die brisante geopolitische Lage Israels im Nahen Osten und die Einschätzung der israelischen Regierung sein, dass sich die angreifenden AkteurInnen durch Attributionssignale in ihrem Handeln nicht beeinflussen lassen. Vergleicht man diese Interpretation des Befundes für Israel mit jenem für die US-Regierung, so zeigt sich, dass sich die USA unter Präsident Trump deutlich häufiger dieses Instrument eingesetzt haben, denn im Durchschnitt wächst die Anzahl der politischen Attributionen von jährlich 4,5 unter Präsident Obama auf 9 während der Präsidentschaft Donald Trumps.

Eine genauere Analyse der IT-Unternehmen als StellvertreterInnen demokratischer Regierungen ergibt folgendes Bild: Tabelle 16 listet zunächst die zehn am häufigsten im Datensatz verzeichneten US-IT-Unternehmen auf. An erster Stelle rangiert FireEye, deren Tochterfirma Mandiant 2013 einen für die Cyberattributionsbranche als „bahnbrechend" zu bezeichnenden Threat Research Bericht mit dem Titel „APT 1: Exposing One of China's Cyber Espionage Units" veröffentlichte (MANDIANT 2013). Dieser Bericht identifizierte nicht nur eine spezifische PLA-Einheit als Auftraggeber der Hackergruppe, sondern benannte auch einzelne Mitglieder, wie Wang Dong (aka „Ugly Gorilla") mit deren jeweiligen Klarnamen. Die in einer US-Anklageschrift von 2014 veröffentlichten Details über APT1 lassen dabei ferner den Schluss zu, dass die US-Behörden im Vorfeld der Anklageerhebung mit Mandiant kooperiert, bzw. Informationen ausgetauscht haben müssen (DoJ 2014). Dieser Befund indiziert, dass der technische Attributionsbericht von Mandiant durch die Offenlegung umfangreicher Evidenzen der anschließenden politischen Attribution - in Form der Anklageschrift - den Weg ebnete und deren Glaubwürdig- und Rechtmäßigkeit untermauern sollte. Dass FireEye zumindest zeitweilig als Proxy der US-Sicherheitsbehörden fungiert hat, wird auch dadurch gestützt, dass das Unternehmen seit 2009 neben anderen US-Unternehmen durch In-Q-Tel gesponsert wird, einem staatlichen Non-Profit-Unternehmen, welches jedoch aus dem CIA-Haushalt finanziert wird. In-Q-Tel investiert vor allem in Technologieunternehmen, deren Produkte als besonders relevant für die US-Geheimdienstarbeit angesehen werden (O`Hara 2005).

Das US-Unternehmen Crowdstrike, Rang fünf auf der Liste, wurde durch die Attribution der russischen Proxy-Gruppierungen Fancy und Cozy Bear im US-Präsidentschaftswahlkampf 2016 bekannt. Das Democratic National Committee beauftragte Crowdstrike, die eigenen Netzwer-

Rang	Unternehmen	Vorkommen im HD-CY.CON
1	FireEye	74
2	Symantec	39
3	Palo Alto	23
4	Recorded Future	17
5	Crowdstrike	16
6	McAfee	10
7	Proofpoint	9
8	Secureworks	7
9	Dragos	7
10	ThreatConnect	6

Tabelle 16: US IT-Unternehmen im HD-CY.CON

Quelle: Eigene Darstellung auf Basis des HD-CY.CON.
Attributionen unterschiedlicher Unternehmen können sich auch auf denselben Fall beziehen.

ke zu schützen, dabei sicherte das Unternehmen aber auch umfangreiche Informationen über das Vorgehen der AngreiferInnen und identifizierte diese schließlich als russische Hackergruppierungen mit Verbindungen zu den Geheimdiensten GRU und SVR (Alperovitch 2016). Zwei Entwicklungen verdeutlichen die Bedeutsamkeit der Stellvertreterfunktion von Crowdstrike in dieser Episode: Zum einen unterließ es die Obama-Administration – aus offensichtlichen politischen Gründen - im Wahlkampf die russischen Angriffe öffentlich zu attribuieren, sodass der technischen Attribution eine stärkere Signalfunktion zukam. Zum anderen beschuldigte US-Präsident Donald Trump das Unternehmen in der Folge, gemeinsam mit der Ukraine technische Beweise auf den DNC-Servern zurück gehalten zu haben, die die Unschuld Russlands hätten beweisen können, vielmehr, so Trump, sei der DNC-Hack/Leak lediglich fingiert gewesen (Bajak 2019). Crowdstrike reagierte mit einer Informationsoffensive über die Zusammenarbeit mit dem DNC, um jedweden Eindruck von Parteilichkeit zu vermeiden (CrowdStrike 2020). Die Episode verdeutlicht geradezu idealtypisch, wie sensitive Informationen über Cyberangriffe zum Gegenstand von Stellvertreterbeziehungen werden, die ihrerseits innen- oder außenpolitisch zur Eskalation von Konflikten beitragen können.

Für Israel verzeichnet unser Datensatz (technische) Attributionen von sieben verschiedenen Unternehmen (Tabelle 17). CheckPoint dominierte dabei das Feld, gefolgt von ClearSky und Cybereason. Die Biografie der Gründer von CheckPoint kann als exemplarisch für die IT-Unternehmen der „Start-Up Nation" Israel betrachtet werden: Nachdem die Gründer jahrelang in der bekannten Militärgeheimdiensteinheit Unit 8200 gedient und sich umfangreiche technische Kenntnisse und Fähigkeiten angeeignet hatten, gründeten Gil Shwed, Shlomo Kramer und Marius Nacht 1993 CheckPoint und machten es zu einem der heute weltweit führenden IT-Unternehmen im Threat Intelligence Bereich (Kannunikova 2021).

Der Personalwechsel zwischen staatlichen Geheimdiensteinheiten und dem IT-Privatsektor, die sog. „Revolving door", ist fester Bestandteil des israelischen Cyberökosystems. Die persönliche Nähe zwischen den führenden IT-Unternehmen und staatlichen Sicherheitsagenturen ist hier so groß wie in kaum einem demokratischen Staat, sodass die Staat-Proxy-Beziehungen besonders eng sind. Israelische IT-Unternehmen beschränken ihre Attributionen aber, ebenso wenig wie US-amerikanische, auf rein nationale Ziele. Vielmehr attribuierten sie mit 20 der insgesamt 31 Attributionen in mehr als der Hälfte

Rang	Unternehmen	Vorkommen im HD-CY.CON
1	Check Point	14
2	ClearSky	9
3	Cybereason*	6
4	AVNET*	1
5	Seculert	1
6	SentinelOne*	1
7	CyberX*	1

Tabelle 17: Israelische IT-Unternehmen im HD-CY.CON

Quelle: Eigene Darstellung auf Basis des HD-CY.CON.
Attributionen unterschiedlicher Unternehmen können sich auch auf denselben Fall beziehen.
**Der Hauptsitz dieser Unternehmen ist zwar (teilweise durch Übernahmen seitens US-Konzernen) mittlerweile in den USA, ihre Gründer sind jedoch Israelis und identifizieren sich und ihr Unternehmen auch noch mit ihrem Herkunftsland (vgl. Magistretti 2017; Div 2018; Williams 2020; IT Times 2020).*

Cyberoperationen im Ausland.[17] Neben dem internationalen Kundenportfolio der Unternehmen könnte eine Erklärung hierfür sein, dass eine technische Attribution gegenüber grundsätzlich rivalisierenden oder feindlichen Staaten wie dem Iran immer im Interesse Israels und israelischer IT-Unternehmen ist, um die technische Resilienz primär anvisierter ZielakteurInnen durch die eigenen Berichte zu stärken.

5.5. Der HD-CY.CON: Eine kritische Reflexion

Dieser Abschnitt beschreibt und reflektiert kritisch die Lücken und systematischen Probleme des HD.CY-CON-Datensatzes. Diese betreffen die potenziell eingeschränkte Repräsentativität der untersuchten Vorfälle, die Erfassung von (geheim gehaltenen) Cyberoperationen, die Erfassung von dynamischen Proxybeziehungen über Zeit und die eindeutige Abgrenzung von einzelnen Cyberoperationen und gestaffelten Cyberoperationskampagnen. Ebenso fehleranfällig ist die Intensitätsmessung von unterschiedlichen Angriffstypen.

Für die Beantwortung der Frage, wie repräsentativ der Datensatz im Hinblick auf Cyberoperationen zu bewerten ist, müssen besonders zwei Aspekte beachtet werden: 1. Die Auswahl potenziell erfasster Quellen und deren Beschaffenheit sowie 2. Die inhaltlichen Inklusionskriterien die darüber entschieden haben, ob ein berichteter Cybervorfall in den Datensatz aufgenommen wurde, oder nicht. Im Rahmen des HD-CY.CON wurde grundlegend ein breites Spektrum an regelmäßig (IT-Unternehmenswebseiten; technische Journale; allgemeine Medienwebseiten) sowie stärker vereinzelt (Webseiten staatlicher Stellen wie Ministerien oder Strafverfolgungsbehörden) über Cybervorfälle berichtenden Quellen berücksichtigt. Der Ansatz war, möglichst eine hohe Zahl an öffentlich gemachten Cybervorfällen in einem ersten Schritt zu identifizieren und diese anschließend auf ihre inhaltliche Relevanz hin zu überprüfen. So wurden etwa technische Berichte und Attributionsaussagen von allein über 40 IT-Unternehmen aus über 20 Ländern erfasst. Aufgrund der mittlerweile stark diffundierten Informationsdynamik in Bezug auf Cybervorfälle wurden darüber hinaus auch weniger „klassische" Quellen verwendet, wie etwa Tweets von IT-Experten, insofern sie relevante Informationen enthielten. Somit kann aus Sicht der berücksichtigten Quellenlage von einer vergleichsweise hohen Repräsentativität der im Datensatz enthaltenen Fälle ausgegangen werden, da sich nicht nur auf bestimmte Quellentypen beschränkt wurde.[18] Da sich der HD-CY.CON ferner jedoch nicht auf sämtliche öffentlich gewordenen Cybervorfälle konzentriert, sondern besonders politisch motivierte und relevante Ereignisse in den Fokus rückt, schränken die beschriebenen Inklusionskriterien das erfasste Sample dementsprechend ein. Daher kann die Repräsentativität des Datensatzes im Hinblick auf öffentlich bekannt gewordene Cybervorfälle ohne die Hinzunahme bestimmter Attribute als dahingehend eingeschränkt bewertet werden.

Unser Datensatz dokumentiert zunächst einmal nur solche Cyberoperationen, die bekannt gemacht werden. Wir können aber gestützt auf Indizien davon ausgehen, dass die „wirkliche Anzahl" bösartiger Operationen deutlich höher liegt. Zum einen beklagen die russische, chinesische u.a. Regierungen immer wieder, zum Ziel von Cyberoperationen geworden zu sein, ohne dass nähere Angaben über Angreifende, Vorgehensweisen, Ziele oder Schäden gemacht wer-

[17] US-IT-Sicherheitsunternehmen attribuierten im Untersuchungszeitraum 217 Operationen, aber nur in etwa einem Drittel der Fälle solche gegen US-Ziele (73).

[18] Das im März 2022 gestartete und durch das Auswärtige Amt sowie das Dänische Außenministerium geförderte Konsortialprojekt „European Repository of Cyber Incidents" baut auf dem HD-CY.CON auf, systematisiert und automatisiert die zuvor noch stärker manuell erfolgte Vorfallrecherche jedoch in sehr viel stärkerem Maße.

den, die sog. „Quasi-Attribution“ (vgl. bspw. für Russland: Sayapin 2021, S. 533) Dabei lassen die Aussagen zahlreicher Whistleblower, u.a. Edward Snowdens, sowie fortwährende Berichte über anhaltende US-Cyberoperation in russischen und chinesischen Netzwerken (Perlroth 2021) die Vermutung zu, dass die US-Regierung oder von ihr beauftragte IT-Unternehmen eine deutlich höhere Anzahl von (bösartigen) Cyberoperationen gegen Ziele in aller Welt geplant und durchgeführt haben, ohne dass die Opfer diese detektiert oder nach Detektion attribuiert haben und somit auch nicht im HD-CY.CON enthalten sein können. Gleiches lässt sich auch für andere westliche Demokratien, u.a. das Vereinigte Königreich, aber auch technisch versierte Autokratien, wie die Islamische Republik Iran, vermuten. Zum anderen zeigen unsere Untersuchungen, dass auf Seiten der Opfer als auch der Angreifenden erhebliche Anreize bestehen, Angriffe als solche oder die näheren Umstände, z. B. Schäden, zu bestreiten, um mögliche weitere negative Folgewirkungen abzuwenden. Wir gehen daher mit erheblicher Konfidenz davon aus, dass die Mehrzahl der im Untersuchungszeitraum durchgeführten Cyberoperationen in unserem Datensatz nicht erfasst werden konnte. Da wir uns dieser Gefahr bewusst waren, haben wir besonderes Augenmerk auf jene Operationen gelegt, die öffentlich attribuiert wurden, weil wir davon ausgingen und ausgehen, dass diese politisch eine stärkere Wirkung entfalten als jene Operationen, die von einer oder beiden Seiten der Konfliktdyade verschwiegen wurden.

Ferner lässt die eingeschränkte Datenlage nur (sehr) tentative Aussagen über die Veränderung der Proxybeziehungen zu staatlichen AuftraggeberInnen über Zeit zu, u.a. weil die betroffenen Organisationen selten freiwillig Auskunft über ihre genauen Auftrags- und Kontrollstrukturen geben. Häufig geben die Kodierungen lediglich jene Zuschreibungen wieder, die die Angegriffenen selbst und/oder Drittinstitutionen, z. B. IT-Sicherheitsfirmen, vornehmen. Unserem Datensatz liegt indes eine sozialkonstruktivistische Interpretationslogik zugrunde, die der Attribution eines Angriffs durch das Opfer oder Dritte, aufgrund der daraus resultierenden Selbstbindung, eine hohe Folgewirkung zuschreibt. So wurde bspw. der APT Fancy Bear seit Beginn der Operationstätigkeit eine besondere Nähe zum russischen Militärgeheimdienst GRU zugeschrieben; seit etwa 2017 sind die Attribuierenden der APT Fancy Bear-Operationen aber (überwiegend) dazu übergegangen, Angriffe dieser Gruppe direkt dem GRU zuzuschreiben.

Über die Schwere der Schäden von Cyberangriffen gibt unser Datensatz nur begründete Schätzungen ab, insbesondere können wir nicht gewährleisten, dass die Opfer von Angriffen wahrheitsgemäß alle Schäden berichten und/oder nur Kenntnis von diesen haben. Angegriffene haben, so eine Ausgangsannahme unseres Projektes, starke Anreize, Operationen überhaupt nicht zu attribuieren oder zumindest deren schädliche Wirkung zu untertreiben, u.a. um Reputationskosten zu vermeiden oder den Angriffsmodus weiter analysieren zu können und daraus ggfs. Gegenmaßnahmen entwickeln zu können (Eichensehr 2020). Würde die Anzahl der Attributionen (weiter) steigen und die rechtliche Spezifizität der Tatbestandsmerkmale in der Begründung der Verantwortungszuweisung weiter ausdifferenziert werden, bspw. um durch die Schaffung internationaler Attributionsstandards das Normwachstum zu beschleunigen (Eichensehr 2019), dann könnte der HD-CY.CON diese Veränderungen erfassen.

Schließlich möchten wir auf ein definitorisches Problem hinweisen, welches potentiell die Anzahl der Operationen als auch deren eskalierende Wirkung betrifft: Einige Cyberoperationen beginnen als Spionageangriffe, können oder werden dann aber später zu anderen Zwecken weiter genutzt, z. B. Sabotage. Kriminelle Ransomware-Angriffe sind hier nur ein Beispiel. Ob und ab wann es sich bei solchen Operationen um Einzelangriffe handelt oder eine geplante Kampagne, ist von außen schwer zu ermessen. Eine Interpretationsweise zielt darauf ab, Cyber-

operationen als das zu interpretieren, was andere AkteurInnen daraus im Sinne der Attribution machen. Wir gehen zudem davon aus, dass die Wahl des Operationstyps mit der asymmetrischen Beziehungskonstellation korreliert: Muss ein Angreifender davon ausgehen, dass der Angegriffene (effektiv) erwidern kann, dann werden die Angriffsziele beschränkter ausgewählt werden, als wenn die Eskalationskosten günstiger für den Angreifenden verteilt sind. Verändern sich jedoch die Interdependenzbeziehungen gravierend, indem manche Staaten ihre Verteidigungsvektoren schließen oder zumindest technisch unzugänglicher machen, aber weiterhin über starke Angriffskapazitäten verfügen, dann könnte die Anzahl längerfristig angelegter Spionage- oder Sabotagekampagnen deutlich ansteigen.

6. Fazit und Perspektiven für die weitere Forschung

Die Anzahl und Qualität der Studien zu Veränderungen von bösartigen Cyberoperationen sind in den vergangenen zwei Jahrzehnten stark angewachsen. Neben technischen, politik- und rechtswissenschaftlichen Analysen finden sich auch immer mehr systematische quantitative Studien, die einen oder mehrere der neu entstandenen Cyberkonfliktdatensätze nutzen.

Die evidenzbasierte Cyberkonfliktforschung steht dennoch gleich in zweifacher Hinsicht noch am Anfang: Zum einen erfassten die bisherigen Datensätze primär staatliches Angriffsverhalten und vernachlässigten nichtstaatliche Akteure sowie das Attributionsverhalten der Staaten; zum anderen veränderten sich Angriffsarten und Ziele der Cyberoperationen so rasch, bspw. im Bereich der kritischen Infrastruktur und Ransomware, sodass die Forschung diese dynamische Entwicklung nicht mehr zeitnah analysieren konnte. Der Datensatz HD-CY.CON setzt hier an, indem er 1.265 Cyberoperationen anhand von 43 Kategorien über den Zeitraum von 2000 bis 2019 erfasst. Die Datensammlung besteht aus einer Excel-basierten tabellarischen Liste von bösartigen Cyberoperationen, welche die Angreifenden (Gruppen/Institutionen), die Angegriffenen, den Modus und das (potentielle) Ziel der Operation, unterschiedliche Zuschreibungsformen von Verantwortung sowie die (geschätzten Schäden) des Angriffs verzeichnen. Den vollständigen Datensatz sowie das Codebuch machen wir über die Datenplattform der Universität Heidelberg zugänglich.[19] Die Fortführung und Erweiterung des Datensatz ist durch Anschlussprojekte bis auf Weiteres gewährleistet. Mit der Fortentwicklung zielen wir primär auf die völker- und europarechtliche Einordnung der Cyberoperationen, i.e. einzelne Tatbestandsmerkmale sowie die weitere Ausdifferenzierung der Attributions- und Sanktionshandlungen der Mitgliedsstaaten der Europäischen Union (vgl. Bendiek und Schulze 2021).

Unsere Datensammlung zeigt ferner, dass die Anzahl der Cyberoperation seit 2000 erheblich angestiegen ist und die Mehrzahl der Operationen bislang von einer überschaubaren Zahl staatlicher aber auch nichtstaatlicher AkteurInnen, sog. Proxies ausgeht. Die Mehrheit der Operationen dienten kriminellen und Spionagezielen, eine Minderheit richtete sich auf die Zerstörung von Daten oder angeschlossenen Systemen. Gemessen an den Fähigkeiten der AkteurInnen, Schaden durch Cyberoperationen zu bewirken, ist das Konfliktintensitätsniveau nach wie vor bemerkenswert moderat (Gesamtdurchschnittsintensität des HD-CY.CON: 1,85 von max. 15 Punkten). Ausnahmen bestätigen die Regel: Im Rahmen von konventionellen Konflikten, insbesondere dem Russland-Ukraine-Konflikt, kam es mehrfach zu Angriffen auf kriti-

[19] Der Datensatz HD.CY-CON und das dazugehörige Codebuch sind frei verfügbar unter: https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB.

sche Infrastruktureinrichtungen; am Ende des Untersuchungszeitraumes ist es mit dem SolarWinds als auch Microsoft-Exchange-Angriffen zu kostenträchtigen Spionageoperationen gegen US-Ziele gekommen. Deutlich erkennbar in unseren Daten ist zudem die Nutzung von sogenannten StellvertreterInnen, die Staaten dazu dienen, ihr Cyberkonfliktverhalten zu verschleiern und dadurch Vorteile im Wettbewerb mit dem jeweiligen Gegner zu erlangen.

Die spezifischen Daten in HD-CY.CON ermöglichen eine detailliertere Analyse von Attributionsprozessen als dies mit den schon verfügbaren Datensätzen möglich war. Indem wir technische von politischen Attributionen trennen und auch deren zeitliche Einordnung vornehmen, ergeben sich mehrere interessante Forschungslinien: Zunächst können quantitative und qualitative Studien untersuchen, inwiefern die von uns festgestellte unterschiedliche Nutzung von Proxies zur Verschleierung von Angriffshandlungen durch autokratische Regime und zur Vermeidung von Attributionshandlungen durch demokratische Regime über Zeit und unterschiedliche Dyadenkonstellationen hinweg stabil ist. Qualitative Studien können insbesondere in den Blick nehmen, ob und inwieweit das hier vorgestellte liberale Erklärungsmodell auch für die offensive Nutzung von Proxies durch demokratische Regierungen tauglich ist. Hier bietet es sich bspw. auch an, mit most-similar oder most-dissimilar Fallstudiendesigns kontrollierte Vergleiche zwischen den Regimetypen und ggfs. Regimesubtypen anzustellen.

Eine zweite Entwicklungslinie für die Cyberkonfliktforschung ergibt sich aus der Zusammenschau von (frühem) Attributionsverhalten und einer möglichen späteren Eskalation. Bislang geht die rezente Konfliktforschung davon aus, dass Geheimhaltung und Verschleierung von Konfliktverhalten durch eine oder beide Konfliktparteien der (erfolgreichen) Eskalationskontrolle dient. Da wir in unserem Datensatz sowohl Konfliktintensitäten von Cyberinteraktionen als auch für bestehende Offline-Konflikte verzeichnen, kann der HD.CY-CON auch für systematische Vergleiche mit einer mittleren oder hohen Fallzahl, z.B. einer Qualitative Comparative Analysis (QCA) genutzt werden, die die Wirkung von Verschleierung oder anderen Konfliktverhaltensparametern untersuchen. Gleiches gilt natürlich auch für Vergleiche, die die unterschiedlichen Angriffsarten in den Fokus rücken.

Ein zweiter wichtiger Themenkomplex, den wir mit dem HD.CY-CON stärker in den Blick nehmen, ist der Einsatz und die Veränderung der Nutzung von Cyberproxies. Könnten wir in den Daten zeigen, dass der Cyberproxyeinsatz über Zeit abnimmt, und würde die Attribution von Cyberoperationen gegenüber staatlichen AkteurInnen so erleichtert werden, so könnte dies zumindest potentiell das Normwachstum beflügeln (Finnemore und Hollis 2016, S. 459). Gleiches gilt für die Zunahme staatlicher Attributionen trotz weiterhin bestehendem Proxygebrauch, i.e. zur technischen Attribution. Eine solche Konstellation könnte auf die (langsame) Entkoppelung der staatlichen Attribution - vor allem in Demokratien – von der Nutzung von IT-Sicherheitsfirmen für die technische Zuschreibung von Cyberoperationen hindeuten, wie wir sie in Ansätzen zum Ende der Amtszeit von Donald Trump in den USA und auch für Europäische Union und ihre Mitgliedstaaten beobachtet haben.[20] Aber auch die Art und Weise des Proxygebrauchs in Autokratien verdient vermehrte Aufmerksamkeit, gibt es doch stichhaltige Hinweise dafür, dass sich deren Beziehung zu den jeweiligen Regierungen verändern kann oder auch deren Vorgehensweise mit jenen krimineller Gruppen korrespondiert, weil MitarbeiterInnen von staatlich-unterstützten Einheiten „nach Dienstschluss" noch eigenen privatwirtschaftlichen Interessen nachgehen. Welche staatlichen Stellvertreterkonstellationen gehen

[20] In diesem konkreten Fall können wir feststellen, dass nicht nur die konfliktdeeskalierende Wirkung von fehlender staatlicher politischer Attribution aufgegeben wurde, sondern mit der Strategie des „persistent engagement" und „forward defense" eine Vorgehensweise gewählt wurde, die den Gegner ständig und proaktiv in den eigenen Netzen in Schach halten soll (Harnisch 2022).

regelmäßig mit kriminellen Aktivitäten ihrer MitarbeiterInnen einher? Unter welchen Umständen bieten staatlich-gestützte Gruppen auch für andere „Kunden" Stellvertreterdienste an? Auch für diese Policy-orientierten Fragestellungen hält der HD.CY-CON die notwendigen Daten für eine evidenzbasierte Analyse bereit.

Schließlich bietet der vorliegende Datensatz auch differenzierte Daten für niedrigschwellige Konfliktintensitäten an. Damit wird der Blick auf die Interaktion zwischen On- und Offlinekonfliktverhalten geschärft. Setzen Cyberoperationen immer zu einem bestimmten Zeitpunkt der Konfliktintensität von Offlinekonflikten ein und ergänzen diese stets Offlineverhalten (Cyberoperationen als abhängige Variable von bestehenden Offlinekonflikten)? Oder substituieren Cyberoperationen Offline-Konfliktverhalten, bspw. wenn durch geografische Distanz Cyberoperationen preiswerter und effektiver erscheinen? Unter welchen Umständen eskalieren Cyberoperationen so weit, dass Offlinekonflikte die Folge sind? (Cyberoperationen als unabhängige Variable für Offlinekonflikte).

Die Weiterentwicklung unseres Datensatzes als auch der bestehenden Sammlungen von Valeriano und Maness sowie des CFR-Trackers bilden eine immer verlässlichere Datenbasis für quantitative und qualitative Untersuchungen des Cyberkonfliktgeschehens. Eingedenk der starken Anreize für die konfliktbeteiligten Parteien Cyberoperationen und ihre Effekte zu verheimlichen, sollten die Datensätze und die aus ihnen gewonnen Erkenntnisse stets vorsichtig interpretiert werden.

7. Anhang

7.1 Aus dem Projekt hervorgegangene Publikationen

Sammelband:

Zettl, Kerstin/Harnisch, Sebastian/Hansel, Mischa (2022): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen, Baden-Baden: Nomos.

Beiträge in einem Sammelband:

Jeweils in: Zettl, Kerstin/Harnisch, Sebastian/Hansel, Mischa (2022): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen, Baden-Baden: Nomos:

- **Harnisch, Sebastian** (2022): Cyber Fiasko: Populismus, proaktive Selbstverteidigung und die gescheiterte Cybersicherheitspolitik der Trump-Regierung.
- **Zettl, Kerstin** (2022a): Der Einsatz von Cyberproxies zur Wahrung autokratischer Regimesicherheit – Iran und Nordkorea im Vergleich.
- **Steiger, Stefan** (2022): Auf leisen Pfoten oder brüllend laut: Chinesische und russische Cyberangriffe im Vergleich.

Harnisch, Sebastian (2020): Spreading Cyber-Autocracy? The Shanghai Cooperation Organization and the Diffusion of Norms of "Internet Sovereignty", in Marianne Kneuer/Thomas Demmelhuber (Hg.): Authoritarian Gravity Centers. A Cross-Regional Study of Authoritarian Promotion and Diffusion, New York: Routledge, 249-274.

Artikel in Fachjournals:

Harnisch, Sebastian/Zettl-Schabath, Kerstin (2022): Secrecy and Norm Emergence in Cyber-

space. The US, China and Russia Interaction and the Governance of Cyber-Espionage. Democracy & Security. DOI: 10.1080/ 17419166. 2022.2097074

Zettl, Kerstin (2021): Macht im Cyberspace: Eine Übersicht der bisherigen Forschung und künftiger Perspektiven anhand des Proxy-Konzepts. Zeitschrift für Friedens- und Konfliktforschung. https://doi.org/10.1007/ s42597-021-00064-2

Konferenzpapiere:

Zettl, Kerstin: "IT-Companies as Defensive Cyber-Proxies? How Democracies Play the Blame-Game in Cyberspace". Paper presented at the Virtual Conference "Conflict Delegation and Proxy Wars in International Security", organized by the Military Academy at ETH Zurich, in cooperation with the Department of Politics and International Relations at the University of Reading, and the Lauder School of Government, Diplomacy & Strategy at the Interdisciplinary Center Herzliya, 23. September 2021.

Harnisch, Sebastian/Zettl, Kerstin (2021). It takes more than a pair: The U.S., China, Russia and the (non-)emergence of a global cyber-espionage norms. Paper for the ISA Annual Convention 2021.

Dissertation:

Zettl, Kerstin (2022b). „Staaten und ihre Stellvertreter im Cyberspace: Ein liberaler Erklärungsansatz autokratischer und demokratischer Cyberproxy-Nutzung", Februar 2022.

Sonstiges:

Harnisch, Sebastian/Zettl, Kerstin (2020). Blame Game im Cyberspace. Informationstechnik als Waffe? in: Ruperto Carola 16.

Zettl, Kerstin (2020): A Brief History of Cyberattacks in 2019, Spotlight-Artikel, in: HIIK: Conflict Barometer 2020. Heidelberger Institut für Internationale Konfliktforschung.

7.2 Verzeichnisse der Abbildungen und Tabellen

Abbildungen

Tabellen

7.3 Literaturverzeichnis

Alperovitch, Dmitri (2016): Bears in the Midst: Intrusion into the Democratic National Committee. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt geprüft am 15.12.2019.

Backes, Oliver; Swab, Andrew (2019): Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. Hg. v. Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states, zuletzt geprüft am 30.11.2021.

Bajak, Frank (2019): Why Trump asked Ukraine's president about 'CrowdStrike'. Hg. v. Associated Press. Online verfügbar unter https://apnews.com/article/trump-impeachment-inquiry-donald-trump-ap-top-news-politics-technology-aa1f66a1770d4995a6bada960a7d119e, zuletzt aktualisiert am 18.10.2019, zuletzt geprüft am 20.08.2021.

Baram, Gil; Sommer, Udi (2019): Covert or not Covert: National Strategies During Cyber Conflicts. In: T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga und G. Visky (Hg.): 11th International Conference on Cyber Conflict: Silent Battle. Tallinn: NATO CCD COE Publications, S. 197–212.

Bartholomew, Brian; Guerrero-Saade, Juan Andres (2016): Wave your flags! Deception tactics muddying attribution in targeted attacks. q. Hg. v. Virus Bulletin Conference.

Behar, Richard (2016): Inside Israel's Secret Startup Machine. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/?sh=27c295f61a51, zuletzt aktualisiert am 30.05.2016, zuletzt geprüft am 11.10.2021.

Bendiek, Annegret; Schulze, Matthias (2021): Attribution als Herausforderung für EU-Cybersanktionen. Hg. v. Stiftung Wissenschaft Und Politik. Online verfügbar unter https://www.swp-berlin.org/publikation/attribution-als-herausforderung-fuer-eu-cybersanktionen.

Berghel, Hal (2017): On the Problem of (Cyber) Attribution. In: Computer 50 (3), S. 84–89. DOI: 10.1109/MC.2017.74.

Bing, Christopher; Taylor, Marisa (2020): Exclusive: China-backed hackers 'targeted COVID-19 vaccine firm Moderna'. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-exclidUSKCN24V38M, zuletzt aktualisiert am 30.07.2020.

Borghard, Erica D.; Lonergan, Shawn W. (2016): Can States Calculate the Risks of Using Cyber Proxies? In: Orbis 60 (3), S. 395–416. DOI: 10.1016/j.orbis.2016.05.009.

Bronk, Christopher; Tikk-Ringas, Eneken (2013): Hack or attack? Shamoon and the Evolution of Cyber Conflict. Hg. v. James A. Baker III Institute for Public Policy. Rice University. Online verfügbar unter https://scholarship.rice.edu/bitstream/handle/1911/92672/ITP-pub-Working-Paper-ShamoonCyberConflict-020113.pdf?sequence=1, zuletzt aktualisiert am 2013, zuletzt geprüft am 03.06.2020.

Buchanan, Ben (2017): The cybersecurity dilemma. Hacking, trust and fear between nations. New York, NY: Oxford University Press.

Buchanan, Ben; Cunningham, Fiona S. (2020): Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis (Fall 2020). In: Texas National Security Review 3 (4), S. 54–81. DOI: 10.26153/tsw/10951.

Calabresi, Massimo (2017): The Secret History

of an Election. In: TIME Magazine 190 (5), S. 32–39.

Carnegie, Allison (2021): Secrecy in International Relations and Foreign Policy. In: Annual Review of Political Science 24, S. 213–233.

Carnegie, Allison; Carson, Austin (2020): Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation: Cambridge University Press.

Carson, Austin (2020): Secret Wars: Covert Conflict in International Politics. Princeton, NJ: Princeton Univ. Press.

Cerulus, Laurens (2019): How Ukraine became a test bed for cyberweaponry. Unter Mitarbeit von Politico. Online verfügbar unter https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/, zuletzt aktualisiert am 14.02.2019, zuletzt geprüft am 16.04.2021.

Chon, Gina; Clover, Charles (2015): US spooks scour China's 5-year plan for hacking clues. Hg. v. Financial Times. Online verfügbar unter https://www.ft.com/content/40dc895a-92c6-11e5-94e6-c5413829caa5, zuletzt aktualisiert am 25.11.2015, zuletzt geprüft am 30.11.2021.

Cohen, Avner (2010): The worst-kept secret: Israel's bargain with the bomb. New York: Columbia University Press.

Collier, Jamie (2017): Proxy actors in the cyber domain: Implications for state strategy. In: St Antony's International Review 13 (1), S. 25–47.

CrowdStrike (2020): Our Work with the DNC: Setting the record straight. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt aktualisiert am 05.06.2020, zuletzt geprüft am 14.04.2021.

Div, Lior (2018): Cybereason named Israel's most promising startup. Hg. v. Cyberreason. Online verfügbar unter https://www.cybereason.com/blog/calcalist-israel-most-proming-start-up, zuletzt aktualisiert am 19.04.2018, zuletzt geprüft am 07.10.2021.

DoJ (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, zuletzt aktualisiert am 22.07.2015, zuletzt geprüft am 23.11.2020.

DoJ (2017a): U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, zuletzt aktualisiert am 21.03.2017, zuletzt geprüft am 15.04.2021.

DoJ (2017b): U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations, zuletzt aktualisiert am 27.11.2017, zuletzt geprüft am 30.11.2021.

DoJ (2021): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion, zuletzt aktualisiert am 19.07.2021, zuletzt geprüft am 01.10.2021.

Eckel, Mike (2019): In Moscow Treason Trial, A Major Scandal For Russian Security Agency. Hg. v. Radio Free Europe. Online verfügbar unter https://www.rferl.org/a/russia-hacker-mikhailov-stoyanov-fsb-scandal-for-russian-security-agency/29794092.html, zuletzt aktualisiert am 27.02.2019, zuletzt geprüft am 30.11.2021.

Edwards, Benjamin; Furnas, Alexander; Forrest, Stephanie; Axelrod, Robert (2017): Strategic aspects of cyberattack, attribution, and blame. In: Proceedings of the National Academy of Sciences of the United States of America 114 (11), S. 2825–2830. DOI: 10.1073/pnas.1700442114.

Egloff, Florian J. (2020): Public attribution of cyber intrusions. In: Journal of Cybersecurity 6 (1), S. 484. DOI: 10.1093/cybsec/tyaa012.

Egloff, Florian J.; Smeets, Max (2021): Publicly attributing cyber attacks: a framework. In: Journal of Strategic Studies, S. 1–32. DOI: 10.1080/01402390.2021.1895117.

Eichensehr, Kristen (2020): The Law & Politics of Cyberattack Attribution. In: UCLA Law Review 67.

Eichensehr, Kristen E. (2019): Decentralized Cyberattack Attribution. In: AJIL Unbound 113, S. 213–217. DOI: 10.1017/aju.2019.33.

Farwell, James P.; Rohozinski, Rafal (2011): Stuxnet and the future of cyber war. In: Survival 53 (1), S. 23–40.

Finnemore, Martha; Hollis, Duncan B. (2016): Constructing norms for global cybersecurity. In: American Journal of International Law 110 (3), S. 425–479.

Gady, Franz-Stefan (2015): New Snowden Documents Reveal Chinese Behind F-35 Hack. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/, zuletzt aktualisiert am 27.01.2015, zuletzt geprüft am 25.05.2021.

Gilli, Andrea; Gilli, Mauro (2019): Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. In: International Security 43 (3), S. 141–189.

Goel, Sanjay; Nussbaum, Brian (2021): Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. In: IEEE Open Journal of the Communications Society 2, S. 1082–1093.

Goertz, Gary; Diehl, Paul F. (1992): The empirical importance of enduring rivalries. In: International Interactions 18 (2), S. 151–163. DOI: 10.1080/03050629208434799.

Gold, Michael (2013): Taiwan a 'testing ground' for Chinese cyber army. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/net-us-taiwan-cyber-idUSBRE96H1C120130719, zuletzt aktualisiert am 19.07.2013, zuletzt geprüft am 29.11.2021.

Goldstein, Lyle J. (2015): Meeting China Halfway. How to Defuse the Emerging US-China Rivalry: Georgetown University Press.

Greenberg, Andy (2019a): Russia's 'Sandworm' Hackers Also Targeted Android Phones. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/sandworm-android-malware/, zuletzt aktualisiert am 21.11.2019, zuletzt geprüft am 10.06.2021.

Greenberg, Andy (2019b): Sandworm. A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. First edition. New York: Doubleday.

Greenberg, Andy (2020): An Elite Spy Group Used 5 Zero-Days to Hack North Koreans. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/north-korea-hacking-zero-

days-google/, zuletzt aktualisiert am 26.03.2020, zuletzt geprüft am 30.11.2021.

Griffiths, James (2019): The great firewall of China. How to build and control an alternative version of the internet. London, Ann Arbor: Zed; ProQuest Ebook Central.

Hansen, Isabella; Lim, Darren J. (2019): Doxing democracy: influencing elections via cyber voter interference. In: Contemporary Politics 25 (2), S. 150–171. DOI: 10.1080/13569775.2018.1493629.

Healey, Jason (2011): The Spectrum of National Responsibility for Cyberattacks. In: The Brown Journal of World Affairs 18 (1), S. 57–70. Online verfügbar unter http://www.jstor.org/stable/24590776.

Healey, Jason (2012): Claiming the Lost Cyber Heritage. In: Strategic Studies Quarterly 6 (3), S. 11–20. Online verfügbar unter https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf.

Hulcoop, Adam; Scott-Railton, John; Tanchak, Peter; Brooks, Matt; Deibert, Ron (2017): Tainted leaks: Disinformation and phishing with a Russian nexus. University of Toronto (Citizen Lab Research Report, 92).

Insikt Group (2019): Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/iranian-cyber-operations-infrastructure/, zuletzt aktualisiert am 26.06.2019, zuletzt geprüft am 29.11.2021.

Insikt Group (2021): Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/, zuletzt aktualisiert am 28.07.2021, zuletzt geprüft am 14.11.2021.

IT Times (2020): Microsoft schluckt israelisches Cybersecurity-Startup CyberX. Hg. v. IT Times. Online verfügbar unter https://www.it-times.de/news/microsoft-schluckt-israelisches-cybersecurity-startup-cyberx-135743/, zuletzt aktualisiert am 22.06.2020, zuletzt geprüft am 03.11.2021.

Joshi, Sahil (2020): Mega Mumbai power outage may be result of cyber attack, final report awaited. Hg. v. India Today. Online verfügbar unter https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20, zuletzt aktualisiert am 20.11.2020, zuletzt geprüft am 23.06.2021.

Kannunikova, Tatiana (2021): Gil Shwed, Co-Founder & CEO of Check Point Software Technologies Ltd | Company & CEO Profile. Hg. v. Gadgets Reviews. Online verfügbar unter https://gadgets-reviews.com/company-ceo-profiles/5706-heck-point-software-technologies.html, zuletzt aktualisiert am 12.05.2021, zuletzt geprüft am 11.10.2021.

Klimburg, Alexander (2011): Mobilising Cyber Power. In: Survival 53 (1), S. 41–60. DOI: 10.1080/00396338.2011.555595.

Lee, Robert (2016): The Problems with Seeking and Avoiding True Attribution to Cyber Attacks. Online verfügbar unter https://www.robertmlee.org/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/, zuletzt aktualisiert am 04.03.2016.

Lin, Herbert (2016): From Soup to Nuts. Attribution of Malicious Cyber Incidents. In: Journal of International Affairs 70 (1), S. 75–137. Online verfügbar unter www.jstor.org/stable/90012598.

Lin, Herbert (2019): The existential threat from cyber-enabled information warfare. In: Bulletin

of the Atomic Scientists 75 (4), S. 187–196.

Lindsay, Jon R. (2013): Stuxnet and the Limits of Cyber Warfare. In: Security Studies 22 (3), S. 365–404. DOI: 10.1080/09636412.2013.816122.

Lindsay, Jon R. (2015): Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. In: Journal of Cybersecurity 1 (1), 53-67. DOI: 10.1093/cybsec/tyv003.

Lohmann, Sarah (2018): Second Roundtable Looks at Role of Private Sector and Civil Society in Attribution – AICGS. Hg. v. American Institute for Contemporary German Studies. John Hopkins University. Online verfügbar unter https://www.aicgs.org/2018/06/second-roundtable-looks-at-role-of-private-sector-and-civil-society-in-attribution/, zuletzt aktualisiert am 28.06.2018, zuletzt geprüft am 18.Ma 2020.

Magistretti, Bérénice (2017): Cybersecurity startup SentinelOne raises $70 million. Hg. v. Venture Beat. Online verfügbar unter https://venturebeat.com/2017/01/25/cybersecurity-startup-sentinelone-raises-70-million/, zuletzt aktualisiert am 25.01.2017, zuletzt geprüft am 03.11.2021.

Manantan, Mark Bryan (2020): The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea. In: Issues & Studies 56 (03), S. 2040013. DOI: 10.1142/S1013251120400135.

MANDIANT (2013): APT1: Exposing one of China's cyber espionage units. Hg. v. MANDIANT. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, zuletzt aktualisiert am 19.02.2013, zuletzt geprüft am 25.05.2021.

Maness, Ryan; Valeriano, Brandon (2016): Cyber spillover conflicts: transitions from cyber conflict to conventional foreign policy disputes? In: Karsten Friis und Jens Ringsmose (Hg.): Conflict in Cyber Space. Theoretical, Strategic and Legal Perspectives. London: Routledge, S. 45–64.

Maschmeyer, Lennart (2021): The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. In: International Security 46 (2), S. 51–90.

Maurer, Tim (2016): 'Proxies' and Cyberspace. In: Journal of Conflict and Security Law 21 (3), S. 383–403. DOI: 10.1093/jcsl/krw015.

Maurer, Tim (2018): Cyber Mercenaries. Cambridge: Cambridge University Press.

Maurer, Tim; Geers, Kenneth (2015): Cyber proxies and the crisis in Ukraine. In: Kenneth Geers (Hg.): Cyber war in perspective. Russian aggression against Ukraine. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, S. 79–86.

Microsoft Threat Intelligence Center (2021): HAFNIUM targeting Exchange Servers with 0-day exploits. Hg. v. Microsoft Security. Online verfügbar unter https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 14.11.2021.

Mueller, Milton; Grindal, Karl; Kuerbis, Brenden; Badiei, Farzaneh (2019): Cyber Attribution. Can a New Institution Achieve Transnational Credibility? In: The Cyber Defense Review 4 (1), S. 107–122.

Novetta (2016): Operation Blockbuster. Unraveling the Long Thread of the Sony Attack. Hg. v. Novetta. Online verfügbar unter https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

O'Hara, Terence (2005): In-Q-Tel, CIA's Venture Arm, Invests in Secrets. Hg. v. The Washington Post. Online verfügbar unter https://www.wa-

shingtonpost.com/wp-dyn/content/article/2005/08/14/AR2005081401108.html, zuletzt aktualisiert am 02.08.2016, zuletzt geprüft am 12.08.2021.

P**erez, Evan** (2016): U.S. official blames Russia for power grid attack in Ukraine - CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html, zuletzt aktualisiert am 12.02.2016, zuletzt geprüft am 29.09.2021.

Perlroth, Nicole (2021): This Is How They Tell Me the World Ends. London: Bloomsbury Publishing.

Poznansky, Michael; Perkoski, Evan (2018): Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution. In: Journal of Global Security Studies 3 (4), S. 402–416.

Proofpoint (2017): Leviathan: Espionage actor spearphishes maritime and defense targets | Proofpoint US. Hg. v. Proofpoint. Online verfügbar unter https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets, zuletzt aktualisiert am 27.01.2019, zuletzt geprüft am 01.07.2021.

Ralston, William (2020): The untold story of a cyberattack, a hospital and a dying woman. Hg. v. Wired. Online verfügbar unter https://www.wired.co.uk/article/ransomware-hospital-death-germany, zuletzt aktualisiert am 11.11.2020, zuletzt geprüft am 29.06.2021.

Rid, Thomas (2013): Cyber war will not take place. Oxford, New York: Oxford University Press. Online verfügbar unter http://lib.myilibrary.**com**/detail.asp?id=557267.

Rid, Thomas; Buchanan, Ben (2015): Attributing Cyber Attacks. In: Journal of Strategic Studies 38 (1-2), S. 4–37. DOI: 10.1080/01402390.2014.977382.

Rollins, John (2015): U.S.-China Cyber Agreement. Hg. v. Congressional Research Service. Library of Congress. (CRS Insight, IN10376). Online verfügbar unter https://www.hsdl.org/?abstract&did=788047.

Romanosky, Sasha; Boudreaux, Benjamin (2019): Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government: RAND Corporation.

Sabbagh, Dan (2021): Experts say China's low-level cyberwar is becoming severe threat. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat, zuletzt aktualisiert am 23.09.2021, zuletzt geprüft am 30.11.2021.

Sayapin, Sergey (2021): Russian approaches to international law and cyberspace. In: Nicholas Tsagourias und Russell Buchan (Hg.): Research Handbook on International Law and Cyberspace. Cheltenham: Edward Elgar Publishing, S. 525–546.

Schulzke, Marcus (2018): The politics of attributing blame for cyberattacks and the costs of uncertainty. In: Perspectives on Politics 16 (4), S. 954–968.

Schwartz, Mathew J. (2017): French Officials Detail 'Fancy Bear' Hack of TV5Monde. Hg. v. Bankinfo Security. Online verfügbar unter https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983, zuletzt aktualisiert am 12.06.2017, zuletzt geprüft am 19.04.2021.

SSU (2021): SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine. Hg. v. Security Service of Ukraine. Online verfügbar unter https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy, zuletzt aktualisiert am 04.11.2021, zuletzt geprüft am 30.11.2021.

Steffens, Timo (2018): Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin: Springer Vieweg.

Stewart, Will (2009): Were Russian security services behind the leak of 'Climategate' emails? Hg. v. Dailymail. Online verfügbar unter https://www.dailymail.co.uk/news/article-1233562/Emails-rocked-climate-change-campaign-leaked-Siberian-closed-city-university-built-KGB.html, zuletzt aktualisiert am 06.12.2009, zuletzt geprüft am 19.05.2021.

Sytas, Andrius (2019): Lithuania fears Russia will attempt to sway its elections. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-lithuania-russia-cyber-idUSKCN1PU1O3, zuletzt aktualisiert am 05.02.2019, zuletzt geprüft am 30.11.2021.

Tucker, Patrick (2018): Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. Hg. v. DefenseOne. Online verfügbar unter https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/, zuletzt aktualisiert am 07.12.2018, zuletzt geprüft am 28.04.2021.

Valeriano, Brandon; Maness, Ryan (2015): Cyber war versus cyber realities. Cyber conflict in the international system. Oxford, New York: Oxford University Press.

Valeriano, Brandon; Maness, Ryan C. (2014): The dynamics of cyber conflict between rival antagonists, 2001–11. In: Journal of Peace Research 51 (3), S. 347–360. DOI: 10.1177/0022343313518940.

Welgan, Jeff (2017): Can data solve cyber's diversity problem? Hg. v. CyberVista. Online verfügbar unter https://www.cybervista.net/corporate-leaders-should-read-chinas-five-year-plan-part-2/, zuletzt aktualisiert am 16.05.2017, zuletzt geprüft am 30.11.2021.

Whittaker, Zack (2019): Mueller report sheds new light on how the Russians hacked the DNC and the Clinton campaign. Hg. v. Techcrunch. Verizon Media. Online verfügbar unter https://techcrunch.com/2019/04/18/mueller-clinton-arizona-hack/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAqdj1iRFophqbdgCGDbfJhH-2o66TTiWR1bI_UPSfACTRMAb0nsOd-Oqplj8M2WiQEzOreez-D6QXpxEEmQHke-GoPYpquBm44kFOM0hhjjO8JRUJXW5NdbnYtF0dRL7Qa7Zq_TxkfcdI5rqXpowhki6VJeYV7oni1P96rwmN5Z0, zuletzt aktualisiert am 18.04.2019, zuletzt geprüft am 13.07.2020.

Weiss Moritz (2021): The rise of cybersecurity warriors?, Small Wars & Insurgencies, DOI: 10.1080/09592318.2021.1976574

Williams, Nick (2020): Rockwell to expand cyber services through acquisition of Israeli company. Hg. v. Milwaukee Business Journal. Online verfügbar unter https://www.bizjournals.com/milwaukee/news/2020/01/08/rockwell-to-expand-cyber-services-through.html, zuletzt aktualisiert am 08.01.2020, zuletzt geprüft am 03.11.2021.

Zettl, Kerstin (2019): Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland. In: Z Außen Sicherheitspolit 12 (4), S. 429–451. DOI: 10.1007/s12399-020-00789-7.

Zhao, Suisheng (2021): The US–China Rivalry in the Emerging Bipolar World: Hostility, Alignment, and Power Balance. In: Journal of Contemporary China, S. 1–17. DOI: 10.1080/10670564.2021.1945733.

Über die Autor*innen

Sebastian Harnisch
Sebastian Harnisch ist Professor für Internationale Beziehungen am Institut für Politische Wissenschaft der Universität Heidelberg. In der Vergangenheit war er Forschungsstipendiat (Seoul National University, Japan Center for International Exchange, Tokio und Institute of East Asia Studies, Columbia University) sowie Gastprofessor an der Al-Farabi-Universität, Almaty, der China Foreign Affairs University, Peking, und der Akademie des Auswärtigen Amts, Berlin. Zu seinen jüngsten Veröffentlichungen gehören "Asymmetrien in Cyberkonflikten" (Baden-Baden: Nomos, 2022).

Kerstin Zettl-Schabath
Kerstin Zettl-Schabath ist wissenschaftliche Mitarbeiterin im Konsortialforschungsprojekt „European Repository on Cyber Incidents", das gegenwärtig vom Auswärtigen Amt und vom dänischen Außenministerium gefördert wird. Zuvor war sie bis 2021 Mitarbeiterin im von der DSF geförderten Projekt „Sicherheit durch Verschleierung: Warum Regierungen Proxies in Cyberkonflikten einsetzen". Ihre bereits eingereichte Dissertation zu autokratischen und demokratischen Cyberproxies baute auf dem darin entstandenen Cyberkonfliktdatensatz HD-CY.CON auf. Sie war zuletzt Mitherausgeberin des Sammelbandes „Asymmetrien in Cyberkonflikten" (Baden-Baden: Nomos, 2022).

DSF
Am Ledenhof 3-5
49074 Osnabrück
+49 541 60035-42
www.bundesstiftung-friedensforschung.de
info@bundesstiftung-friedensforschung.de
ISSN 2193-794X