Z Friedens und Konflforsch (2022) 11:65–90
https://doi.org/10.1007/s42597-021-00064-2

LITERATURBERICHT

Macht im Cyberspace: Eine Übersicht der bisherigen Forschung und künftiger Perspektiven anhand des Proxy-Konzepts

Kerstin Zettl

Eingegangen: 8. September 2020 / Überarbeitet: 19. August 2021 / Angenommen: 29. September 2021 / Online publiziert: 22. Oktober 2021

Zusammenfassung Entgegen seiner ursprünglichen Gründungshistorie erscheint das Internet zunehmend seitens staatlicher Akteure instrumentalisiert zu werden. Vor allem Autokratien nutzen dabei verstärkt den Cyberspace als offensiven Konfliktaustragungsraum. Jedoch entwickelten auch demokratische Staaten vor allem auf Grundlage ihrer technologischen Überlegenheit genuine Machtressourcen im digitalen Raum. Der vorliegende Literaturbericht liefert eine Analyse des bisherigen Zugangs der politikwissenschaftlichen Forschungslandschaft zu Macht im Cyberspace. Bisherige Konzeptualisierungen werden miteinander verglichen und zu einem integrativen Modell zusammengefügt, welches zwischen Machtressourcen und Machtfunktionen differenziert. Für deren empirische Sichtbarmachung wird das Konzept des Proxys zunächst hinsichtlich seiner theoretischen Implikationen diskutiert und im Folgenden als analytische Referenzkategorie für die Diskussion spezifischer Debatten um Macht im Cyberspace verwendet. Diese beziehen sich erstens auf die Nutzung offensiver Cyberproxies seitens autokratischer Staaten, zweitens auf die Instrumentalisierung defensiver Cyberproxies seitens demokratischer Staaten und drittens auf die jeweilige Rolle staatlicher Proxies für beide Regimetypen im Rahmen einer Agenda-Setting-Funktion auf internationaler Ebene. Dabei wird jeweils zwischen den zwei benannten Kategorien auf der Hard- sowie Softpower-Ebene unterschieden, wodurch die eingeschränkte, in Teilen jedoch vorhandene Bedeutung materieller Machtfunktionen, welche durch Proxies im Cyberspace verfolgt werden können, expliziter herausgearbeitet werden kann. Macht im Cyberspace bezieht sich in allen drei empirischen Themenfeldern überwiegend auf Informationen als zentrale Ressource, welche vor allem zur Manipulation bestehender Asymmetrien gegenüber externen sowie internen Akteuren seitens autokratischer und demokratischer Regierungen variant zum Einsatz kommt. Dabei spielt Macht zur offensiven

Kerstin Zettl (✉)
Institut für Politische Wissenschaft, Universität Heidelberg, Heidelberg, Deutschland
E-Mail: kerstin.zettl@ipw.uni-heidelberg.de

sowie defensiven Eskalationskontrolle im Rahmen von Konflikten eine bedeutende Rolle, jedoch auch Machtressourcen nichtstaatlicher Akteure, welche auf die diskursive Beeinflussung internationaler Verregelungsbemühungen des Cyberspace als Konfliktaustragungsraum ausgerichtet sind.

Schlüsselwörter Macht · Cyberspace · Proxies · Attribution · Eskalation · Agenda-Setting

"Power in cyberspace: a review of previous research and future perspectives using the proxy concept."

Abstract Contrary to its original founding history, the Internet appears to be increasingly instrumentalized by state actors. Autocracies, in particular, are increasingly using cyberspace as a space for offensive conflict resolution. However, democratic states have also developed genuine power resources in digital space, primarily on the basis of their technological superiority. This literature review provides an analysis of the political science research landscape's approach to power in cyberspace to date. Previous conceptualizations are compared and combined into an integrative model that differentiates mainly between power resources and power functions. To make these empirically visible, the proxy-concept is first discussed in terms of its theoretical implications and then used as an analytical reference category for discussing specific debates about power in cyberspace. These relate firstly to the use of offensive cyber proxies by autocratic states, secondly to the instrumentalization of defensive cyber proxies by democratic states, and thirdly to the respective role of state proxies for both regime types in the context of an agenda-setting function at the international level. In each case, a distinction is made between the two categories at the hard and soft power level, which makes it possible to more explicitly elaborate the limited, but in part existing, significance of material power functions that can be pursued by proxies in cyberspace. In all three empirical fields, power in cyberspace refers predominantly to information as a central resource, which is used primarily to manipulate existing asymmetries vis-à-vis external and internal actors on the part of autocratic and democratic governments. In this context, power plays an important role for offensive as well as defensive escalation control in the context of conflicts, but also power resources of non-state actors, which are aimed at discursively influencing international efforts to regulate cyberspace as a conflict resolution domain.

Keywords Power · Cyberspace · Proxies · Attribution · Escalation · Agenda-Setting

1 Einführung: Der Cyberspace als Konfliktaustragungsraum und welche Rolle Macht darin spielt

> „Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

Als John Perry Barlow (1996) mit diesen Worten seine *„Declaration of the Independence of Cyberspace"* veröffentlichte, brachte er die mit dem Internet verbundene Hoffnung der IT-Entwicklergemeinde zum Ausdruck, damit einen vor allmächtigen Staaten geschützten Kommunikations- und Handlungsraum geschaffen zu haben. Fast ein Vierteljahrhundert später scheint es dagegen, als ob sich ein Großteil der Befürchtungen der damaligen Internetpioniere weitestgehend bewahrheitet hätte, blickt man auf die wissenschaftlichen Debatten rund um staatliche Überwachungs-, Zensur- und Kontrollmaßnahmen im digitalen Raum (Deibert 2009; Klimburg 2011; King et al. 2013; Inglis 2019).

Auch wenn man das Forschungsfeld auf den immer stärker im Fokus stehenden Bereich der Cyberkonfliktforschung[1] eingrenzt, erscheint der Cyberspace zunehmend staatlich dominiert (z. B. Gartzke 2013; Valeriano und Maness 2015; Blank 2017; Nye 2018), analog vor allem zur autokratischen *Internet Governance* (Rød Geelmuyden und Weidmann 2015; Kendall-Taylor et al. 2020). Staaten scheinen somit die primär machtvollen Akteure im Rahmen von Cyberkonflikten zu sein. Dieser Befund wurde in bestimmten Kontexten jedoch auch angezweifelt, definiert man Macht nicht ausschließlich über materielle Kapazitäten und Befugnisse: So zeigten etwa Studien zum Arabischen Frühling, wie zivilgesellschaftliche Akteure[2] trotz bestehender Zensurmaßnahmen verschlüsselte Messengerdienste im Rahmen der innerstaatlichen Konflikte nutzten, um ihr eigenes Mobilisierungspotenzial und somit ihre Machtposition gegenüber staatlichen Stellen zu verbessern (Allagui und Kuebler 2011; Pierskalla und Hollenbach 2013). Aber auch die Informationsdienste selbst, als transnational agierende Privatunternehmen, können zunehmend Einfluss auf bestehende Konflikte nehmen, indem sie verstärkt als erste Informationsquelle hierzu auftreten und auch für die Konfliktakteure selbst zum wichtigen Kommunikationstool geworden sind (Zeitzoff 2017). Die Macht privater Unternehmen kann sogar so weit reichen, dass sie politische Amtsinhaber von ihren Plattformen und daher einem bedeutenden, öffentlichen Diskursraum ausschließen können, was somit ihre in den letzten Jahren gestiegene Diskursmacht begründet (Roose 2021). Nicht zuletzt zeigt die Corona-Pandemie, auf welche Weise digitale Technologien

[1] Damit sind solche Forschungsarbeiten gemeint, welche sich mit genuin im digitalen Raum stattfindenden Konfliktinteraktionen vor allem, aber nicht nur staatlicher Akteure auseinandersetzen. Cyberkonflikte werden zumeist im Sinne von Hacking-Operationen verstanden, welche die CIA-Triade der Informationssicherheit der betroffenen Systeme verletzen (*Confidentiality, Integrity, Availability*), können jedoch zuweilen auch Desinformationskampagnen miterfassen.

[2] Für eine bessere Lesbarkeit wird in diesem Text das generische Maskulin verwendet. Die entsprechenden Formulierungen umfassen jedoch in gleichem Maße weibliche und männliche Personen.

auch Kriminelle ermächtigen können, um ihre finanziellen Ziele zu erreichen (Buil-Gil et al. 2020).

Diese kurze Gegenüberstellung macht deutlich, dass Macht im Cyberspace ein multidimensionales Phänomen zu sein scheint, im Hinblick auf die damit verbundenen Akteursebenen, Funktionen und Effekte, sowie auftretenden Formen von Machtpotenzialen. Der vorliegende Text kann dabei nur einen Versuch darstellen, den Macht-Cyberproxy-Nexus theoretisch erschließen und anschließend empirisch anzuwenden, ohne dabei Vollständigkeit für sich beanspruchen zu können.

Der vorliegende Bericht hat somit das Ziel, die bisherige Darstellung und Konzeptualisierung von Macht im Cyberspace aufzuarbeiten und dabei bislang existierende Widersprüche und Herausforderungen zu identifizieren. Hierfür werden zunächst unterschiedliche Machtdefinitionen aus Sicht der in erster Linie politikwissenschaftlichen Forschung im Cyberkontext vorgestellt und miteinander verglichen. Darauf aufbauend wird ein integratives Konzeptualisierungsschema von Macht im Cyberspace entwickelt, mit der Hard- vs. Softpower-Differenzierung auf der einen, sowie der Unterscheidung zwischen Machtressourcen und Machtformen auf der anderen Achse.[3] In einem künstlich kreierten Konfliktaustragungsraum wie dem Internet kann eine sinnvolle Machtdefinition nicht beschränkt sein auf physisch sichtbare Auswirkungen und Machtmittel, weshalb ein besonderer Fokus auf unterschiedliche *Machtformen* im digitalen Raum gelegt wird.

Daran anschließend wird plausibilisiert, warum für eine Diskussion dieser theoretischen Annahmen in Bezug auf *Cybermacht* im Kontext aktueller Problemfelder der internationalen Politik das Konzept des *Proxys*, sowohl im Sinne einer Akteurschaft als auch einer rein technischen Stellvertretung, als analytische Referenzkategorie gewählt wird. Mit dieser als Fixpunkt werden sodann unterschiedliche Machtformen und -mittel im Rahmen konkreter, empirischer Handlungs- und Problemfelder entsprechend der aktuellen Forschungsliteratur unterschieden und bestehende Forschungslücken, sowie Entwicklungspotenziale betont. Die konkreten Empirie-Themenfelder lassen sich direkt aus den zuvor dargelegten theoretischen Erwägungen der Macht-Debatte im digitalen Raum ableiten und mit Hilfe des Proxy-Konzepts daran zurückbinden. Dabei geht es zum einen um materielle Macht im Rahmen staatlichen Eskalationsmanagements im Cyberspace mit Hilfe offensiver Proxies als Akteuren, zweitens um staatliches Eskalationsmanagement im Cyberspace mit Hilfe defensiver Proxies als Akteuren, sowie um die Macht des Agenda-Settings auf internationaler Ebene, mit einem stärkeren Fokus auf Normentwicklungsprozesse, sowie transnationale Diskurse über die „richtige“ Form von Global Governance im digitalen Raum.

[3] Hierfür sowie für den Bericht allgemein werden überwiegend, jedoch notwendigerweise nicht ausschließlich Beiträge aus peer-review-Ausgaben politikwissenschaftlicher Fachjournale betrachtet, auch, um aktuellere Themenfelder bearbeiten zu können. Der Schwerpunkt liegt dabei auf den Fachbereichen Internationale Beziehungen, aber auch Strategic Studies, sowie der immer prominenter werdenden Cyberkonfliktforschung. Da letztere jedoch noch nicht so etabliert ist wie die konventionelle Konfliktforschung, ist es geboten, auch anderweitige Veröffentlichungsformate, bei entsprechender, inhaltlicher Güte, in die Analyse miteinzubeziehen, welche ebenfalls direkte oder indirekte Implikationen für die Konzeptualisierung und Analyse von Macht im Cyberspace aufweisen.

Ein abschließendes Fazit führt die einzelnen Abschnitte zusammen und identifiziert darauf aufbauend sinnvolle Anknüpfungspunkte für künftige Forschungsvorhaben zur Thematik.

2 Machtdefinitionen im Cyberspace

Eine der wohl verbreitetsten Definitionen von Macht lieferte bislang Max Weber. Darin definiert er diese als „jede Chance innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht" (Weber 1972, S. 28). Ähnlich argumentierte auch Joseph Nye, indem er konstatierte, dass *„[…] power is the ability to affect the outcomes you want, and if necessary, to change the behaviour of others to make this happen"* (Nye 2002, S. 4). Zentral sind somit drei Aspekte: Erstens die jeweiligen Ziele des machtausübenden Akteurs, zweitens der Umstand, dass er diese auch gegen den Willen anderer Akteure umsetzen kann, und drittens die *potenzielle* Notwendigkeit, deren Verhalten hierfür ändern zu müssen. Nye prägte darüber hinaus mit seiner Unterscheidung zwischen *Hard-* und *Softpower* die politikwissenschaftliche Debatte um Macht nachhaltig. *Hardpower* versteht er dabei stärker als eine realistische, auf militärisch-materielle Ressourcen beschränkte Machtkonzeption, bei der ein Gegenüber durch Zwang zu einer Handlung (oder einem Unterlassen) gezwungen wird. *Softpower* dagegen orientiert sich stärker an einer liberalen Lesart von Macht, bei der es darum geht, den Gegenüber davon zu *überzeugen*, dass seine Ziele und Wünsche mit den eigenen übereinstimmen (Nye 1990, S. 166). Somit kann dieser Ansatz eher als Macht durch Überzeugung oder Anziehung beschrieben werden. 2010 übertrug Nye seine Dichotomie dann auch auf den Cyberspace, indem er sie mit den sogenannten *„three faces of power"* der Politikwissenschaften verknüpfte (Nye 2010, S. 7): Erstens einer handlungsinduzierenden Macht, zweitens einer handlungsverhindernden Macht und drittens einer Macht durch Agenda-Kontrolle, ermöglicht vor allem auch durch Abschreckung (Nye 2010, S. 2).

Eine weitere, auch für den Cyberspace womöglich opportune Kategorisierung differenziert zudem zwischen der *„power to destroy, the power to produce and exchange, and the power to integrate […]"* (Boulding 1990, S. 10), welche sich ebenfalls an das *Hard* vs. *Softpower*-Konzept anbinden ließe. Über diese binäre Kategorisierung hinaus geht dabei sowohl konzeptuell als auch methodisch der *Cyber-Power-Index* des *Belfer Center* der *Harvard Kennedy School*, der einen der bislang seltenen Versuche unternimmt, staatliche Machtpotenziale im Cyberspace auf verschiedenen Ebenen zu messen und in einen quantifizierbaren Index zu überführen. So sind machtvolle Handlungen im Cyberspace eben nicht nur auf die Zerstörung fremder Infrastrukturen, oder die Manipulation fremder Informationssysteme ausgerichtet, sondern können auch defensiv oder ökonomisch motiviert sein, sowie die Formung und Etablierung normativer Standards auf internationaler Ebene zum Ziel haben (Voo et al. 2020). Dabei wird trotz des Fokus auf staatliche Akteure ein gesamtstaatlicher Ansatz verwendet, weshalb vor allem auch Machtpotenziale domestischer Akteure in die jeweiligen Werte ihrer Länder mit einfließen. Dies entspricht stärker dem sogenannten *„whole-of-nation"*-Ansatz, welcher bereits an anderer Stelle

für den Cyberspace und die darin stattfindende Machtdistribution diskutiert wurde (Klimburg 2010). Einen ähnlichen Ansatz verfolgt auch der 2021 veröffentlichte Bericht des *International Institute for Strategic Studies* (IISS) mit dem Titel *„Cyber Capabilities and National Power: A Net Assessment"*. Darin werden potente Cyberstaaten anhand ihrer Fähigkeiten in drei Machtebenen eingeteilt, mit einzig den USA auf der *„Tier One"*. Der IISS-Bericht ist im Gegensatz zum Index-basierten Vorgehen des Belfer Center qualitativ geprägt und erfasst noch stärker das breitere Cyber-Ökosystem der jeweiligen Staaten (IISS 2021).

Im Hinblick auf zur Anwendung kommende Machtressourcen argumentierte Tim Stevens (2018) am Beispiel der Verregelung von *„Cyberweapons"*, dass die hierbei wirkenden Machtformen weniger aus feststehenden, bestimmten Akteuren zugeschriebenen Machtquellen resultieren, sondern Ausdruck ihrer relationalen Wirkung auf das Verhalten anderer sei. Daher könne die Kategorisierung der Macht als *„compulsory, institutional, structural, and productive"* von Barnett und Duvall (2005) auch auf Handlungen den Cyberspace betreffend übertragen werden. Die vier Formen unterscheiden dabei vor allem zwischen direkten und indirekten Machtformen über andere Akteure, durch die spezifischen oder diffusen Interaktionsbeziehungen zu diesen (*compulsory vs. institutional*). Strukturelle Macht dagegen versteht sich als Ausdruck der Konstitution der jeweiligen Akteurskapazitäten in direkten Beziehungen miteinander. Zuletzt fügt sich produktive Macht am ehesten in den Bereich der *Überzeugung durch Anziehung*-Logik des Softpower-Konzepts ein: Hierbei steht die diffuse Produktion subjektiv geteilter Bedeutungszuweisungen, somit gemeinsamer Verständnisse in sozialen Systemen im Vordergrund (Barnett und Duvall 2005, S. 43).

Auf Grundlage dieser theoretischen Kategorisierungen wird folgendes Schema zur Analyse von Macht im Cyberspace vorgeschlagen:

Die grundlegende Hauptunterteilung in Hard- und Softpower erscheint auch für den Cyberspace als Handlungsfeld sinnvoll, da somit zwischen materieller Zwangsmacht, sowie stärker auch auf immateriellen Dynamiken basierender Überzeugungsmacht unterschieden werden kann. Auch die drei Kategorien von Kenneth Boulding können hierüber erfasst werden. Gerade in einer künstlich erschaffenen Domäne wie dem Cyberspace, mit einem Fokus auf den grenzüberschreitenden Austausch von Informationen, erscheint die Betrachtung nur einer der beiden Aspekte unzureichend und würde die steigenden Verquickungen der Online- und Offline-Ebene in nahezu allen Politikbereichen nicht adäquat reflektieren, welche schon länger als zentrale Besonderheit des Mediums herausgestellt werden (Hansen und Nissenbaum 2009, S. 1161). Auf der horizontalen Achse dagegen drücken die Kategorien der Machtressourcen und Machtfunktionen aus, was Nye mit seiner Hinzunahme der *„three faces of power"* in seiner Arbeit aus 2010 im Sinn hatte: Aufzuzeigen, dass z. B. ein und dieselbe Hard- oder Softpower-Ressource ganz unterschiedliche Machtfunktionen bedienen kann und somit stets der Kontext ihrer Anwendung für die Analyse ihrer tatsächlichen Wirkung von Bedeutung ist.

Die einzelnen Felder der Matrix werden nun nochmal im Detail anhand kurzer Beispiele erklärt: Beginnend mit den möglichen Ressourcen von Hardpower im Cyberspace, wird hierbei die Unterscheidung zwischen Hard- und Software als materielle Ressourcen, sowie Personen als menschliche Ressourcen deutlich. Alle drei

können sowohl von Staaten, jedoch auch privaten Akteuren wie Firmen genutzt werden, um Zwangsgewalt in unterschiedlichen Kontexten auszuüben. Beispiele wären die Kontrolle über ISPs (Deibert 2009), Zero-Day-Exploits (J. Carr 2011, S. 152), sowie Hacker mit entsprechender Expertise (Klimburg 2011).

Damit auf der Ebene der Hardpower verbundene Funktionen der machtvollen Nutzung dieser Ressourcen wäre etwa der Einsatz einer disruptiven Malware in Netzen des Gegners (z. B. Stuxnet), um diesen zu einer Verhaltensänderung zu bewegen, oder auch ein staatlich gelenkter Internet-Shutdown während innerstaatlicher Proteste (Handlungsverhinderung).[4] Die tatsächlichen Zwangspotenziale offensiver Cybertools wurden jedoch bereits angezweifelt (Maness und Valeriano 2016; Borghard und Lonergan 2017).[5] So scheinen etwa Angriffe auf kritische Infrastrukturen allenfalls als Substitutionen zu konventionellen Militäreinsätzen zu fungieren, mit fehlender, direkter Wirkung auf diese (Kostyuk und Zhukov 2019).

Softpower-Ressourcen im Cyberspace wären vor allem Normen, wie sie z. B. die staatliche Sorgfaltspflicht (*Due Diligence*; Liu Yuying 2017) im digitalen Raum darstellt. Aus liberaler Sicht können zudem Interessenkompatibilitäten oder auch Interdependenzen genutzt werden, um andere Akteure von etwas zu überzeugen. Ein Beispiel wäre die Notwendigkeit eines hinreichend freien und transnationalen Internets, zur Stärkung der eigenen, ökonomischen Interessen. Softpower-Funktionen im Hinblick auf eine angestrebte Verhaltensänderung des Gegenübers wären dagegen beispielsweise staatliche IT-Zertifizierungsprogramme, um Konsumenten dazu zu bringen, ausschließlich zertifizierte Produkte zu verwenden. Handlungsverhinderung auf der Softpower-Ebene könnte dagegen durch *Naming-und-Shaming-*, bzw. *Accusation*-Strategien, in internationalen Organisationen angestrebt werden, um einen Normbrecher durch das Offenlegen des Normbruchs durch potenzielle Reputationsverluste in Zukunft hiervon abzubringen (Finnemore und Hollis 2020). Ein Beispiel hierfür wären Anklageerhebungen gegen ausländische Hacker, mit rechtlicher Fundierung: Deren materielle Zwangswirkung ist oftmals eingeschränkt, jedoch können sie erhebliche Signalwirkungen auf normativer Ebene entfalten (Hinck und Maurer 2019).

Im Folgenden wird erläutert, warum Proxies für eine empirische Anwendung dieser aufgezeigten Machtkonzeption im Rahmen aktueller Konflikte im Bereich des Cyberspace ein sinnvolles Konzept darstellen.

3 Cyberproxies in der Forschung: Ausdruck ambivalenter Cybermacht-Konzeptualisierungen

Die Übertragung des in der analogen Konfliktforschung weithin verwendeten Proxy-Konzepts (u. a. Ladwig III 2008; Maoz und Şan-Akca 2012; Mumford 2013; Berman

[4] Das kurzfristige Ausspielen solch materieller Hardpower-Differentiale im Sinne einer realistischen Machtkonzeption, könnte langfristig jedoch ebenso zu größeren Kosten, als Gewinnen für die jeweilige Regierung führen.

[5] Zudem müssen offensive Cybertools für das Eindringen in gut geschützte Ziele maßgeschneidert sein, weshalb kein Äquivalent für ein durch rein physische Gewalt erobertes Offline-Ziel existiert (Libicki 2009, S. 119).

und Lake 2019) in den digitalen Konfliktaustragungsraum, erfolgte vor allem seit Mitte der 2010-er Jahre durch die Forschungsgemeinde. Die bisherigen Arbeiten zum Thema beschäftigten sich in erster Linie mit der Beziehung zwischen einem *staatlichen Auftraggeber* und einem *nichtstaatlichen Agenten* im Cyberspace, da dies die primär untersuchungswürdige Konstellation sei (Schmitt und Vihul 2014; Maurer 2016, 2018a, b; Borghard und Lonergan 2016; Canfil 2016).[6] Tim Maurer versteht unter einem Cyberproxy einen *„intermediary that conducts or directly contributes to an offensive action that is enabled knowingly, actively or passively, by a beneficiary"* (2018a, S. 31). Terme wie *„Patriotic Hackers", „Cyber Criminals"* (Klimburg 2011), *„Cyber-Mercenaries"* (Maurer 2018a) oder *„Cyber-Militias"* (Harris 2008; Ottis 2011) sind dabei regelmäßig enger an das Proxy-Konzept angebunden als etwa *„Netizens"* (Hauben und Hauben 1998), *„White/Grey Hats"* (Kirsch 2014) oder *„Ethical Hackers"* (Palmer 2001), welchen eine größere Unabhängigkeit von staatlichen Stellen nachgesagt wird.[7]

Auch wenn die Mehrzahl der politikwissenschaftlichen Arbeiten mit dem Begriff eine Akteurschaft assoziiert, findet er auch Verwendung im Sinne technologischer Hilfsmittel bzw. Stellvertreter, wie zum Beispiel Drohnen, oder Proxyservern (Malley 2019). Somit werden für den weiteren Verlauf des Berichts Proxies als Akteure, als auch als technische Stellvertreter von Bedeutung sein. In der bisherigen Forschungslandschaft zu Cyberproxies dominierten zwei Perspektiven: Erstens die Konzeptualisierung der Staat-Proxy-Beziehungsformen (Borghard und Lonergan 2016; Maurer 2016, 2018a; Collier 2017; Egloff 2018), sowie zweitens deren völkerrechtliche Bewertung im Hinblick auf das Konzept der *Due Diligence* (Tsagourias 2012; Rivera 2015; Jensen und Watts 2017; Roguski 2020).

Diskutiert man Proxies als Akteure sowie als technische Hilfsmittel im Kontext des Schaubilds aus Tab. 1, zeigt sich, dass das Konzept für jede der einzelnen Kategorien im Hinblick auf den Cyberspace potenzielle Anknüpfungspunkte liefert. Anders gesagt, kann die analytische Nutzung des Proxy-Konzepts dabei helfen, unterschiedliche Machtressourcen- und -formen in der Empirie erst sichtbar zu machen:

Auf der Ebene der Hardpower stellen Proxies vor allem als Akteure wichtige Machtressourcen für Staaten dar. So können die in Tab. 1 als Beispiele genannten ISPs vor allem für autokratische Regierungen im Rahmen nationaler Konflikte als Proxies fungieren, indem sie stellvertretend für diese den Zugang der Oppositionsgruppen zum Internet einschränken. Aufgrund der stärkeren Hardpower-Ressourcen, welche autokratische Regime gegenüber ihren ISPs haben, wird deren Handlungsautonomie als geringer eingeschätzt als bei ISPs in demokratischen Ländern und somit das Risiko, dass sie sich auch gegen den eigenen Staat wenden könnten.

[6] Für den analogen Bereich demonstrierten Assaf Moghadam und Michel Wyss (2020) jedoch, dass auch nichtstaatliche Akteure stärker politische Proxies regelmäßig zu ihrem eigenen Vorteil nutzen. Dass dies auch für den Cyberspace zunehmend der Fall sein könnte, legen diverse technische Berichte der letzten Jahre nahe (Kaspersky 2020; Blackberry 2020).

[7] Alexander Klimburg argumentierte (2011) jedoch für China, dass das Regime gezielt *Netizens* kooptieren würde, um diese ideologisch an das Regime zu binden und ihr Coup-Gefährdungspotenzial zu minimieren.

Tab. 1 Ein integratives Analyseschema für Macht im Cyberspace

–	Machtressourcen	Machtfunktionen
Hardpower	Hardware (z. B. Kontrolle über Internet Service Provider (ISP) etc.) Software (z. B. Zero-Day-Exploits) Personal (z. B. Hacker)	Verhaltensänderung (z. B. disruptiver Malware-Einsatz) Handlungsverhinderung (z. B. Internet-Shutdown während Protesten)
Softpower	Normen (z. B. *Due Diligence*) Interessenskompatibilitäten (z. B. ökonomische Stärke durch Digitalisierung)	Verhaltensänderung (z. B. IT-Zertifizierungsprogramme) Handlungsverhinderung (z. B. *Naming and Shaming*)

Eigene Darstellung

Zudem können offensive Hackergruppen eine wichtige, personelle Ressource für staatlichen Konfliktaustrag darstellen, vor allem, falls es dem jeweiligen Staat an entsprechenden, eigenen Cyberkapazitäten und Fähigkeiten mangelt. In diese Rolle können patriotische Hacker, private *Hacking-for-Hire*-Firmen sowie vor allem jedoch auch Cyberkriminelle schlüpfen (Boeke und Broeders 2018, S. 83). Private IT-Firmen fungieren zudem als potenzielle, defensive Proxies im Rahmen von Attributionsprozessen (vgl. Harnisch und Zettl 2020): Indem sie beispielsweise auf Sicherheitslücken hinweisen, die eine potenzielle Bedrohung für nationale Akteure darstellen können, reduzieren sie somit das oftmals für Regierungen wirkende Dilemma im Hinblick auf die zu vermeidende Offenlegung eigener Attributionsevidenzen und -vektoren (Steffens 2018, S. 141–43). Auf der Softpower-Ebene können wiederum vor allem zivilgesellschaftliche Akteure stellvertretend für Staaten Normentwicklungsprozesse vorantreiben und somit als Machtressource fungieren, etwa indem sie Bewusstsein für emergierende Bedrohungslagen im digitalen Raum schaffen oder Normbrüche offenlegen (z. B. Siemens im Rahmen der *„Charta of Trust"*). Durch wirtschaftliche Verflechtungen können private Unternehmen ihren Regierungen indirekt zudem dabei helfen, Druck auf andere Staaten auszuüben, indem sie Interessenskompatibilitäten mit deren Unternehmen und somit transnationale Interdependenzen schaffen, welche nicht so ohne weiteres ignoriert werden können.[8]

Analog zu den in Tab. 1 unterschiedenen Machtfunktionen werden Proxies im Cyberspace vor allem als Akteure genutzt, um eine Verhaltensänderung herbeizuführen. Die Bedeutung von Proxy-Hackern hinsichtlich dieser Funktion belegt nicht zuletzt die einschlägige Forschung zu autokratischen Cyberproxies, welche vor allem auch immer stärker deren Einsatz im Rahmen von *„cyber-enabled information operations"* betont (Lin 2019), die auf Verhaltensänderungen demokratischer Gesellschaften, z. B. im Rahmen von Wahlen ausgerichtet sein können. Entsprechend der Konzeptualisierung von ISPs als Proxies ist zudem deren implizierte Machtfunktion, im Sinne einer Handlungsverhinderung als Beispiel zu nennen, wenn es darum geht, die Mobilisierungs- und Organisationsmöglichkeiten nationaler Proteste einzuschränken. Verhaltensänderungen auf der Softpower-Ebene können dagegen etwa von IT-Firmen als Proxies vorgenommen werden: Deren Machtfunktion bezieht sich dabei beispielsweise auf das Setzen technischer Beweisführungsstandards,

[8] In der Forschungsliteratur wurde hierfür bereits der Begriff *„Weaponized Interdependence"* geprägt (Drezner et al. 2021).

denen öffentliche Attributionsprozesse entsprechen müssen (Eichensehr 2019). Wie zivilgesellschaftliche Akteure auch, können IT-Firmen zudem durch ihre technischen Berichte Normbrüche vor allem staatlicher Akteure im Cyberspace stellvertretend für ihre Regierungen offenlegen: Diese *Naming-and-Shaming*-Strategie führt zwar zumeist nicht zu einer Sanktionierung der *Non-Compliance*, kann die betroffenen Akteure dennoch künftig davon abhalten, entsprechendes Verhalten zu wiederholen.[9] Neben der Verhaltensänderung sowie Handlungsverhinderung ist jedoch auch das Ausnutzen asymmetrischer Verwundbarkeiten eine weitere, wichtige Funktion autokratischer Cyberproxies. So bereichert sich die nordkoreanische Hackergruppierung Lazarus seit Jahren an westlichen Banken, Unternehmen, Finanzdienstleistern sowie Kryptowährungen, um letztlich das Atomwaffenprogramm des Landes zu finanzieren (Lyngaas 2021). Der digitale Angriffsvektor westlicher Demokratien bildet somit die Machtressource einer auf digitaler Ebene stark abgeschotteten Autokratie, um die Stärkung ihrer militärischen Kernmachtressource trotz internationaler Sanktionen weiterhin gewährleisten zu können.

Wichtig ist im Hinblick an die Anschlussfähigkeit des Konzeptes an die traditionelle Proxy-Forschung jedoch auch die Betrachtung der unterschiedlichen Machtbeziehungen zwischen Auftraggebern und ihren Proxies selbst: Entsprechend des für Spione entwickelten „MICE"-Akronyms, *Money, Ideology, Coercion* und *Ego* können die für den Proxy aus der Beziehung zum Auftraggeber resultierenden Vorteile ausdifferenziert werden. *„Money"* spielt dabei vor allem für *„hacking-for-hire"*-Unternehmen eine bedeutende Rolle, die eine kommerziell-anmutende Beziehung zu ihren Auftraggebern aufweisen (z. B. Ransomware-Gangs wie REvil oder DarkSide, denen zumindest die Duldung seitens russischer Sicherheitsbehörden unterstellt wird; Sanger 2021). Gleichzeitig legen Berichte über das sog. *„Moonlighting"* chinesischer Staatshacker nahe, dass Proxies ihre technischen Machtressourcen auch für eigenmotivierte Machtfunktionen, in diesem Fall dem profitorientierten Hacken „in der Nacht" missbrauchen können (DoJ 2020a). Ideologische Motive können dagegen vor allem die Proxy-Rollenübernahme von sog. *„Patriotischen Hackern"* erklären: Hierbei verfügt der Auftraggeber über eine immaterielle Softpowerressource gegenüber den nichtstaatlichen Akteuren, nämlich der ideologischen Gesinnungskonvergenz mit diesen. Oftmals reichen bereits verbale Äußerungen aus, um die Proxies zu ihren Handlungen im Sinne des Regimes zu bewegen. Ein Beispiel hierfür ist die *Syrian Electronic Armee*, welcher zwar nicht unbedingt eine direkte staatliche Unterstützung oder Anleitung, jedoch ideologischer Zuspruch und auch Duldung seitens Assads unterstellt wird (Warren und Leitch 2016). Gleichzeitig resultiert aus dieser oftmals loseren Beziehungsform für die staatlichen Auftraggeber jedoch auch die Gefahr eines zumindest temporären Kontrollverlustes gegenüber dieser Art von Proxies, wenn deren Handlungen zu eskalativer Natur sind, oder aber eine Art Eigenleben entwickeln (Borghard und Lonergan 2016, S. 406).

Der dritte Beziehungsaspekt der *„Coercion"* entspricht dagegen am stärksten der materiellen Hardpower-Komponente des Akronyms. Gerade russischen Cyberkriminellen gehen oftmals eine Art Tauschhandel mit den nationalen Geheimdiensten

[9] Auf diese Aspekte wird im späteren Abschnitt über defensive Cyberproxies nochmals genauer eingegangen.

ein: Solange sie keine russischen Ziele angreifen und ab und an im Auftrag der Sicherheitsbehörden hacken, können sie auch unbehelligt weiter agieren. Dass deren *Cybercrime*-Operationen jedoch auch gegenüber ausländischen Zielen offenbar den Interessen der eigenen Regierung gefährlich werden können, zeigt das Beispiel der erwähnten DarkSide-Gruppierung. Nachdem diese im Mai 2021 eine große Ölpipeline der USA für mehrere Tage arbeitsunfähig hinterließ, indem die Daten der Firma mit Hilfe einer Erpressungssoftware verschlüsselt wurden, verschwand die Gruppierung in der Folge von der Bildfläche. Experten vermuten, dass der politische Druck der Biden-Administration hierfür verantwortlich gewesen sein könnte, weshalb wohl auch der Kreml, bzw. die russischen Geheimdienste selbst ihre Hardpower-Machtressourcen gegenüber der Gruppierung zur Anwendung gebracht haben könnten (Sanger 2021). Eine weitere Theorie vermutet dagegen stärker eine Anwendung der US-Machtpotenziale im Cyberspace als verantwortlich für das Verschwinden der Cybercrime-Gruppierung (Wolff 2021), die tatsächliche Ursache blieb jedoch bislang unklar.

Zuletzt spielt für viele Hacker das *Ego* eine wichtige Rolle bei der Proxy-Rollenübernahme. Staaten können ihnen wesentlich umfassendere technische Möglichkeiten für ihre Aktivitäten eröffnen, etwa indem sie sie mit *Zero-Day-Exploits* beliefern, eine Praxis, welche etwa für das chinesische Ministerium für Staatssicherheit und deren Proxies bereits berichtet wurde (DoJ 2020b). Aber auch bei den erwähnten IT-Unternehmen, deren Proxyfunktion nicht das Hacking, sondern das Attribuieren ist, kann das Ego, bzw. die eigene Reputation für die Proxyrollenübernahme sprechen.

Im Folgenden werden diese Überlegungen anhand verschiedener empirischer Problem- und Handlungsfelder diskutiert: Die varianten Cyberproxies veranschaulichen dabei die mehrdimensionale Konzeptualisierung von Macht im Cyberspace und verdeutlichen deren Relevanz für spezifische Themen im Rahmen politischer Konflikte.

4 Offensive Cyberproxies im Rahmen von Konflikten: Staatliches Eskalationsmanagement auf der Angreiferseite als Machtfunktion

Zunächst wird Macht im Cyberspace im empirischen Handlungsfeld staatlichen Konfliktaustrags thematisiert, anhand der Rolle, welche offensive Proxies hierbei spielen. Dabei wird aufgezeigt, wie vor allem autokratische Staaten durch deren Einsatz bislang versuchen, Eskalationsmanagement gegenüber im Offline-Bereich militärisch überlegenen Demokratien zu betreiben. Eskalationsmanagement wird somit als eine verbindende Oberkategorie zwischen offensiven und defensiven Cyberproxies eingeführt, um die unterschiedlichen Wirkweisen der Machtfunktionen im Sinne der Verhaltensänderung sowie Handlungsverhinderung besser miteinander vergleichen zu können.

In Abgrenzung zur Logik analog agierender Proxies belegen immer mehr empirische Arbeiten, dass (hauptsächlich) autokratische Staaten nationale Hacker anheuern, anstatt die Mission an ausländische Akteure auszulagern (für *Iran*: Anderson und Sadjadpour 2018; *Russland:* Carr 2011; Maurer und Geers 2015; Connell und

Vogler 2017; *China*: Raud 2015).[10] Auch wenn der digitale Raum in gewisser Weise einer entgrenzten Logik folgt, setzen Staaten somit auch im Cyberspace oftmals auf nationale Machtressourcen, über die sie eine direktere Kontrolle besitzen. Gerade aufgrund der Entgrenzung des Cyberspace erscheint aus operativer Sicht für die Durchführung der meisten Cyberangriffe eine Stationierung des Proxys im Zielland schlicht nicht notwendig. Gleichzeitig wird jedoch die Schaffung einer *„plausible deniability",* einer vorgegebenen Distanz zum Proxy und die hiermit verbundene Verantwortlichkeitsverschleierung oftmals als deren zentrale Machtfunktion angesehen (Canfil 2016). Dies ermöglicht Staaten, welche in konventionellen Konflikten den jeweiligen Kontrahenten unterlegen wären, den Cyberspace als Raum für ihren asymmetrischen Konfliktaustrag zu nutzen. Asymmetrisch insofern, als dass Autokratien oftmals auf der digitalen Ebene weniger verwundbar sind, als Demokratien und sie deren hier größeren Angriffsvektor somit zum eigenen Vorteil nutzen können, um ihre eigenen, asymmetrischen Verwundbarkeiten auf der Offline-Ebene somit auszugleichen.[11] Sie setzen digitale Stellvertreter daher gezielt ein, um Eskalationsmanagement durch die Verantwortlichkeitsverschleierung der eigenen Cyberoperationen zu betreiben, welche hierfür zudem knapp unterhalb der Schwelle kriegsähnlicher Auswirkungen erfolgen (Borghard und Lonergan 2019, S. 137).

Neben dieser eher liberal geprägten Machtfunktion offensiver Cyberproxies demonstrierten empirische Studien der letzten Jahre zudem direkt deren verhaltensändernden oder handlungsverhindernden Machtfunktionen: Für Russland zeigten dabei Benjamin Jensen, Brandon Valeriano und Ryan Maness (2019) auf, welch unterschiedliche Strategien autokratische Staaten mit den ihnen zugeordneten Proxygruppierungen verfolgen können. Das ehemalige Sowjetreich zeichnet sich laut Autoren dabei insbesondere durch den vom KGB-ererbten Pfad des *„information war"* aus, mit Hilfe der lange Zeit als Proxy attribuierten Hackereinheit Fancy Bear (auch bekannt als APT28) und deren *„hack-and-leak"*-Operation während des US-Wahlkampfes 2016 (Shires 2019; Zettl 2020). Auch der Iran unterhält Beziehungen zu unterschiedlichen Cyberproxies, wobei der Fokus dabei bislang auf politischer Cyberspionage gegen Ziele in der Region, sowie disruptiveren Cyberoperationen wie etwa sog. *Wiper*-Attacken gegen saudi-arabische Ziele lag (Bronk und Tikk-Ringas 2013). Im Gegensatz dazu setzt China seine Cyberproxies überwiegend für wirtschaftliche, aber auch politische Spionage ein. Die Effektivität dieses Diebstahls geistigen Eigentums zur Steigerung der wirtschaftlichen Entwicklung des Landes wurde jedoch zuletzt seitens der Forschung zunehmend angezweifelt und somit auch deren spezifische Machtfunktion (Gilli und Gilli 2019). Das Beispiel Nordkoreas verdeutlicht zudem, wie Staaten Proxies im Cyberspace verwenden können, um etwa die negativen Externalitäten politischer und wirtschaftlicher Sanktionen zu umgehen: Durch das erpresserische Erbeuten von Kryptowährung (sog. *Ransomware*-Attacken) zur Finanzierung des eigenen Nuklearwaffenprogramms (Pinkston 2020).

[10] Die bekannteste Ausnahme von dieser Praxis ist Nordkorea, welches vor allem in China, Indien und Russland stationierte Proxies für Cyberattacken nutzt (Insikt Group 2017).

[11] Asymmetrien werden verstanden als ungleichgewichtige Beziehungsmuster, in welchen der weniger abhängige Akteur durch deren Verstetigung einen Vorteil erhalten *kann* (Womack 2016; Long 2017).

Ein genauerer Vergleich der hier angesprochenen Autokratien und deren Cyberproxy-Nutzung lässt jedoch erahnen, dass dabei unterschiedliche Machtressourcen, sowie -funktionen am Wirken sind: Während Russland und China nationale Proxies noch stärker zur Vortäuschung angeblicher Nichtbeteiligung und somit des Eskalationsmanagements instrumentalisieren, trotz bestehender, staatlicher Ressourcen im Cyberbereich, stellt vor allem auch für den Iran der nationale IT-Sektor eine wichtige Ressource dar, um die inhaltlichen Machtfunktionen auf digitaler Ebene überhaupt realisieren zu können. Demgegenüber ist für Nordkorea immer mehr fraglich, inwiefern sich hier angesichts des nationalen Intranets als ausschließlichem Elitenprojekt überhaupt plausibel von Cyberstellvertretern sprechen lässt, da diese für ihre Tätigkeiten entsprechenden Zugriff zu digitalen Ressourcen benötigen (Maurer 2018b). Da das Kim-Regime die digitalen Hardpowerressourcen noch stärker auf der staatlichen Ebene konzentriert, kann es jedoch gleichzeitig die potenziellen Machtfunktionen tatsächlicher Cyberproxies, vor allem auf der Ebene der Softpower, nicht nutzen.

Hinsichtlich der Rolle von Cyberproxies in gewaltsamen Konflikten lässt sich folgender Befund der Cyberkonfliktforschung konstatieren: „Cyberwaffen“[12] und somit auch deren Einsatz durch Cyberproxies spielten bislang beispielsweise in Russlands Georgienfeldzug oder auch dem Ukrainekonflikt seit 2014 lediglich eine substituierende Rolle auf operativer Ebene (Schulze 2020, S. 189). Kostyuk und Zhukov (2019) belegten dies in einer der bislang seltenen, quantitativen Studien zur Thematik für sowohl den Ukraine-, als auch den Syrienkrieg. Somit ist bislang noch kein Fall bekannt, in dem ein Land ein anderes ausschließlich auf digitaler Ebene „besiegt“, dieses also etwa zur Niederlegung von Waffen oder aber zu einer Gebietsabtretung gebracht hätte (Libicki 2009, S. 59, S. 140). Durch Cyberoperationen können demnach (bislang) keine konfliktentscheidenden Verhaltensänderungen beim Gegner hervorgerufen werden, das Machtpotenzial von Cyberproxies ist in diesem Kontext somit eingeschränkt. Jedoch zeigte das russische Beispiel im Georgienkrieg 2008, dass Cyberangriffe wie DDoS-Attacken im Sinne der Kommunikationsstörung des militärischen Gegners untereinander sowie mit der Öffentlichkeit zumindest auf dieser Ebene eine potenziell bedeutsame Rolle im Konfliktverlauf spielen können (Deibert et al. 2012). Gleiches belegten Lutscher et al. (2020) für den Einsatz von DoS-Attacken autokratischer Regime während Wahlen, mit dem Ziel im Ausland stationierte oppositionelle Medienkanäle in ihrer Berichterstattung zu stören. Eine ähnliche Machtfunktionslogik erfüllen zudem die bereits thematisierten ISPs für autokratische Regime im Rahmen domestischer Unruhen, welche den Zugang Oppositioneller zum Internet einschränken können (Kendall-Taylor et al. 2020). Somit scheinen offensive Cyberproxies effektiver Softpower-Machtfunktionen im Rahmen bereits eskalierter Offline-Konflikte zu erfüllen, im Gegensatz zu angestrebten Verhaltensänderungen des militärischen Gegenübers, mit Hilfe von Hardpower-Methoden wie dem Einsatz disruptiver Malware. Die Entwicklungen der letzten Jahre zwischen dem Iran, Israel und den USA legen jedoch zumindest für diesen Konflikt

[12] Die Verwendung dieses Begriffes wird kritisch gesehen, da es sich hierbei im Kern um Software-Code handelt, der eben nicht zwingend zu konfliktiven Handlungen eingesetzt werden muss, wie es etwa bei konventionellen Feuerwaffen der Fall ist.

gleichzeitig nahe, dass sich dies auf taktischer Ebene geändert haben könnte (vgl. Shires und McGetrick 2021, S. 10).

Im Verbund mit der Debatte um die Effektivität russischer *Hack-and-Leak*-Operationen in demokratischen Wahlen, sollten die Machtfunktionen offensiver Cyberproxies seitens künftiger Forschung noch stärker im Rahmen informationsbasierter Verhaltensänderungen untersucht werden. Dabei sollte stärker analysiert werden, auf welche Weise offensive Cyberproxies, wie etwa die sog. „Internet-Trolle" die Zersetzung des öffentlichen Diskurses in liberal-demokratischen Ländern weiter vorantreiben und somit die demokratische Legitimationsgrundlage demokratischer Regierungen als Kern-Softpowerressource stetig errodieren lassen. Cyberangriffe vermögen es bislang eben nicht primär durch physische Gewalt einen Kontrahenten, bzw. dessen Bevölkerung in seinen Handlungen zu manipulieren, sondern vor allem durch den Einsatz polarisierender, Vertrauen unterminierender Cyberinformationsoperationen (Gioe 2018). Informationsasymmetrien zwischen Staaten sowie diesen und ihren Gesellschaften sollten dabei aus theoretischer Perspektive zunehmend in den Fokus genommen werden, da über diese der Einsatz unterschiedlicher Proxies, zum Zwecke unterschiedlicher Machtfunktionen systematischer herausgearbeitet werden könnte.

5 Defensive Cyberproxies im Rahmen von Konflikten: Staatliches Eskalationsmanagement auf der Verteidigerseite als Machtfunktion

Vor allem Staaten können Cyberproxies jedoch nicht nur in der Rolle des Angreifers instrumentalisieren: Auch als Opfer digitaler Aggressionen oder Beeinflussungsversuche können nichtstaatliche Akteure, wie etwa IT-Unternehmen, oder auch Betreiber kritischer Infrastrukturen Staaten helfen, die angestrebte Machtfunktion offensiver Cyberproxies autokratischer Staaten zu entschärfen. Eskalationsmanagement durch den Einsatz defensiver Cyberproxies steht somit im Fokus dieses Kapitels.

Die „Spielregeln" des öffentlichen Cyberattributionsprozesses erfuhren in den letzten Jahren vor allem seitens der politikwissenschaftlichen Forschung eine immer größere Aufmerksamkeit und hiermit verbunden auch die Rolle von IT-Unternehmen darin (Floyd 2018; Poznansky und Perkoski 2018; Baram und Sommer 2019; Egloff 2020). Trotz der auf staatlicher Seite mittlerweile erheblich vorhandenen Cyberattributionsfähigkeiten legen Staaten dennoch nach wie vor in vielen Fällen eine Art Attributionszurückhaltung an den Tag, bzw. überlassen in vielen Fällen privaten Unternehmen die Aufgabe der Verantwortungszuweisung (Romanosky 2017; Eichensehr 2017; Mueller et al. 2019).[13] Erklärt werden kann dies durch den zumindest zeitweilig anzunehmenden Status privater IT-Unternehmen als defensive Cyberproxies vor allem demokratischer Staaten, um in der Rolle der zumeist Angegriffenen

[13] Gleichzeitig verweisen Mueller et al. jedoch auch auf erhebliche Unterschiede hinsichtlich staatlicher Attributionsfähigkeiten, weshalb die Autoren für eine intendierte Diffusion staatlicher Cyberattributionsressourcen plädieren, um Machtasymmetrien langfristig auszugleichen (Mueller et al. 2019).

ebenfalls Eskalationsmanagement zu betreiben.[14] Um im Falle offensiver Cyberoperationen seitens autokratischer Proxies einerseits dem Kontrahenten signalisieren zu können, dass man sehr wohl über dessen Verantwortlichkeit im Bilde ist, gleichzeitig jedoch dem Reaktionsdruck in Folge einer eigenen, politischen Attribution zu entgehen, können somit IT-Unternehmen stellvertretend für demokratische Regierungen diese *Signaling*-Funktion übernehmen. Eskalationsmanagement bedeutet in diesem Fall somit, dass auf der konventionellen Ebene militärisch mächtigere Staaten aus verschiedenen Gründen davor zurückschrecken, einen Cyberkonflikt weiter eskalieren zu lassen. So ist für demokratische Regierungen nach wie vor oftmals nicht klar, wie auf unterschiedlichste Cyberoperationen autokratischer Kontrahenten angemessen und effektiv reagiert werden könnte. Sogenannte *Hack-Backs* scheinen wie aufgezeigt nur in seltenen Fällen realistische Potenziale zur Verhaltensänderung oder -abschreckung eines Akteurs bereit zu halten (Libicki 2018). Diese werden zudem auch hinsichtlich potenzieller Kollateralschäden sowie ungewollter Eskalationsdynamiken als riskant eingestuft, was sich vor allem auch an den bislang z. B. auch von den USA weitestgehend negierten Forderungen privater Unternehmen nach digitaler Selbstjustiz durch private *Hack-Backs* zeigt (Williams 2021). Zur effektiven Aufweichung des eigenen, rechtlich zugesicherten Gewaltmonopols im Cyberspace sind demokratische Regierungen bislang noch nicht bereit, wohl auch, um gegenüber dominanten und einflussreichen Großkonzernen nicht noch mehr Machtressourcen einbüßen zu müssen.

Analoge Gegenmaßnahmen wie z. B. Sanktionen treffen zudem oftmals die verantwortlichen Akteure nicht in ausreichendem Maße (Kwon 2016). Darüber hinaus haben auch demokratische Regierungen, trotz der prinzipiellen militärischen Überlegenheit zumeist kein Interesse daran, einen gewaltsamen Konflikt mit einer Autokratie zu beginnen, entsprechend demokratischer Verantwortlichkeitsverpflichtungen gegenüber der eigenen Bevölkerung, welche die Kosten eines Krieges primär zu tragen hätte und daher oftmals als entsprechend kriegsavers bezeichnet wird. Letzteres erklärt zudem die Entwicklung automatisierter Waffensysteme (z. B. Drohnen) als technische Proxies, welche zwar in den eigenen Kampfverbänden die Opferzahlen senken, gleichzeitig jedoch auf der Seite des Gegners vor allem auch zu zivilen Opfern führen können (Schörnig und Lembcke 2006).

Zwar können privatwirtschaftliche Attributionen demokratischen Regierungen etwas zeitlichen Spielraum gegenüber den Forderungen der eigenen Bevölkerung und der Opposition verschaffen, dennoch erscheinen die weiteren Machtfunktionen dieser Proxy-Attribution im Hinblick auf rechtlich legitimierte Gegenmaßnahmen eingeschränkt. So kann eine privatwirtschaftliche Attribution zwar eine gewisse Zeit das politische Attributionsvakuum überdecken, entbindet die betroffene Regierung jedoch langfristig nicht davon, vor allem auf wiederholte Cyberoperationen desselben Akteurs auch selbst zu reagieren. Wie effektiv stellvertretende Attribution für Staaten im Hinblick auf die angestrebte Verhaltensänderung des autokratischen Angreifers sein kann, hängt dabei von dessen Cyberstrategie ab: Während das durch

[14] Dabei erfordert es jedoch noch weitergehende Forschung etwa dazu, in welche Stufe des von Jason Healey (2011) vorgeschlagenen Spektrums staatlicher Verantwortlichkeit im Cyberspace sich diese Staat-Proxy-Beziehungsform einsortieren lässt.

die IT-Firma FireEye erfolgte Offenlegen chinesischer Cyberspionage gegenüber ökonomischen Zielen 2014 für die USA eine wichtige Machtfunktion zwecks der angestrebten Verhaltensänderung Chinas erfüllte, verfehlten privatwirtschaftliche Attributionen der russischen Wahlbeeinflussung 2016 (etwa durch Crowdstrike) einen ähnlichen Effekt. Grund hierfür war, dass Cyberspionage verdeckt stattfinden sollte, um die angestrebte Machtfunktion zu erfüllen, was im Falle einer öffentlichkeitswirksamen Wahlbeeinflussung durch *Hack-and-Leak*-Operationen nicht der Fall ist. Daher hängt die Effizienz der IT-Firmen als defensive Machtressource auch von der Funktionslogik der offensiven Cyberproxy-Nutzung autokratischer Regierungen ab.[15]

Weitere Akteure, die als defensive Machtressourcen für Staaten im Cyberspace angesehen werden könnten, sind zudem die Betreiber kritischer Infrastrukturen. Diese können stellvertretend für staatliche Behörden wichtige Schutzfunktionen übernehmen. Ähnlich wie im Falle der Attribution geht es hierbei neben der Stärkung der IT-Sicherheit der Systeme auch darum, gesellschaftlichen Handlungserwartungen vorzubeugen, etwa indem im Rahmen von *Public-Private-Partnerships* (PPP) ein großer Teil der Schutzverantwortung für kritische Infrastrukturen an private Betreiber ausgelagert wird (Christensen und Petersen 2017). Beide Seiten ziehen Vorteile aus diesem Arrangement, was ein wichtiges Kriterium für das Auftraggeber-Proxy-Konzept darstellt. Falls kritische Infrastrukturen durch Cyberoperationen angegriffen werden, können Staaten auf die Schutzverantwortung deren privater Betreiber verweisen und verschaffen sich analog zum Attributionsprozess somit einen gewissen Handlungsspielraum gegenüber zivilgesellschaftlichen Akteuren. Gleichzeitig wird die Effektivität dieser handlungsverhindernden Machtfunktion jedoch dadurch auf die Probe gestellt, dass Privatunternehmen die Schutzverantwortung vor allem hinsichtlich bedeutender Bedrohungen für die nationale Sicherheit im Rahmen einer PPP beim Staat sehen (Carr 2016, S. 57). Macht auf der Softpower-Ebene bedeutet hierbei somit in erster Linie den domestischen Diskurs über Rechte und Pflichten zum eigenen Vorteil zu prägen. Stark ermächtigte Proxies können dabei, wie im Offensivbereich jedoch auch, langfristig auch zur Gefahr für staatliche Auftraggeber werden, insofern die negativen Externalitäten der Beziehung aus ihrer Sicht zu stark bei ihnen angesiedelt sind.[16]

6 Agenda-Setting durch Proxies auf internationaler Ebene als Machtfunktion

Proxies können auch auf internationaler Ebene für Staaten unterschiedliche Machtfunktionen bedienen. Seit Ende der 1990-er Jahre wird auf der UN-Ebene darum

[15] Neben diesem *Signaling*-Effekt können stellvertretende Attributionen jedoch auch ganz konkrete Resilienzfunktionen zum Schutz nationaler Infrastrukturen erfüllen, etwa in dem das Bewusstsein oder die Kenntnis über bestimmte Angriffsvektoren bei diesen gestärkt wird (Egloff und Smeets 2021, S. 7).

[16] Für offensive Proxies könnte dies im Falle zunehmender Einschränkungen durch Sanktionen anderer Länder bedeuten, dass die Kosten der Proxyrollen-Übernahme deren positiven Anreize überwiegen könnten.

gerungen, wie sich das Konfliktpotenzial des digitalen Raums effektiver verregeln lässt und somit auch das Anarchieproblem im internationalen System. Der transnationale Charakter des künstlich erschaffenen Cyberspace erfordert dabei umso mehr eine globale *Governance*-Strategie, welche die steigenden Interdependenzen unterschiedlichster Akteure im digitalen Raum entsprechend erfasst. Proxies sind dabei auf demokratischer Seite eine Machtressource im Rahmen dieser *Global Governance*-Bemühungen, etwa indem private Akteure wie Unternehmen oder NGOs verstärkt als Norm-Entrepreneure im Cyberspace auftreten (Hurel und Lobato 2018). Somit können sie Regierungen zum einen die Initiativbürde im Normentwicklungsprozess abnehmen, indem sie als Agenda-Setter fungieren. Andererseits stellen sie auch einen machtvollen Hebel im Konflikt mit autokratischen Staaten auf internationaler Ebene dar: Entsprechend des von den meisten Demokratien propagierten *Multistakeholder*-Ansatzes agieren zivilgesellschaftliche Akteure als Gegenpol zu den staatlichen Ermächtigungsbestrebungen autokratischer Staaten wie Russland oder China (Bendiek und Porter 2013; Strickling und Hill 2017). Indem sie aktiv am Cyberregulationsprozess auf internationaler Ebene teilnehmen, liefern sie ihren demokratischen Regierungen vor allem Softpower-Ressourcen auf der Diskursebene, um steigenden Nationalisierungstendenzen im digitalen Raum entgegen zu wirken.[17] Somit werden derlei Initiativen unterstützt um zu verhindern, dass autokratische Staaten durch einen immer stärkeren staatlichen Zugriff auf digitale Infrastrukturen zu umfangreiche Hardpower-Ressourcen erlangen. Eingebettet ist dieser Gegensatz zudem in den diskursiven Machtkampf um die Konzepte *„information security"* vs. *„cyber security"*: Während Autokratien spezifische Inhalte von Informationen vor allem auf domestischer Ebene als potenzielle Gefahr ansehen und auf nationaler Ebene bereits eingeführte Zensur- und Kontrollmaßnahmen durch internationale Abkommen legitimieren wollen (Hansel et al. 2018), vertreten die meisten Demokratien stattdessen einen Ansatz, bei dem es primär um den Schutz der technischen Systeme geht und nicht um deren Gefahrenpotenziale im Hinblick auf die eigene Regimesicherheit (Mueller 2020).

Hinzu kommt, dass auch autokratische Regierungen entsprechend des sogenannten „Innovationsdilemmas" nicht mehr umhinkönnen, ihre eigene Wirtschaft zunehmend auch auf digitaler Ebene zu stärken, wofür ein gewisses Maß an Interkonnektivität und somit fehlendem staatlichen Einfluss hierauf notwendig ist (Göbel 2012). Somit stellen demokratische Unternehmen durch ihre ökonomischen Verflechtungen mit autokratischen Firmen Interdependenzen sowie Interessenskompatibilitäten her, welche die Anreize für konsequent konfliktives Verhalten der autokratischen Regierungen reduzieren. Dem liegt die theoretische Annahme zu Grunde, dass in asymmetrischen Machtbeziehungen prinzipiell auch der materiell schwächer gestellte Akteur die Beziehung zum eigenen Vorteil nutzen kann, jedoch nur solange, wie er auch die geringere Bedürftigkeit für das besagte Gut aufweist, somit die geringere Präferenzintensität (Keohane 1984, S. 94). Ist dies wie im Falle technologisch-ökonomischer Fortentwicklung für Autokratien nicht mehr der Fall, ist die asymmetrische Machtbeziehung auch nicht mehr zu deren Vorteil ausgestaltet.

[17] Beispiele wären u. a. die *„Charter of Trust"* von Siemens, der unter der Leitung von Microsoft initiierte *„Cybersecurity Tech Accord",* oder auch die *„Global Commission on the Stability of Cyberspace"*.

Gleichwohl gilt auch im Falle „internationaler Cyberproxies“, dass deren Tätigkeiten nur solange die Macht demokratischer Staaten stärken, solange sie im Einklang mit deren Interessen agieren. Decken NGOs beispielsweise demokratische Versäumnisse im Rahmen von Überwachungstechnologieexporten an autokratische Staaten auf, welche deren diskursiven Softpower-Ressourcen schwächen könnten, spricht weniger für die Funktionslogik einer Staat-Proxy-Beziehung (vgl. Amnesty International 2021). Hier wird wie im Falle patriotischer Hacker deutlich, dass der Faktor der *„Ideology“* als Motivation für die Proxy-Rollenübernahme die wohl größte Gefahr des Kontrollverlustes der Staaten über diese Machtressource birgt.

Am Beispiel Chinas wird jedoch auch für wirtschaftlich erfolgreiche Autokratien deutlich, welche wichtige Rolle deren *„Global Player“* im Bereich der Technologieindustrie spielen können. Weltweit erfolgreiche Unternehmen wie Alibaba, Tencent oder speziell auch Huawei können der Volksrepublik dabei helfen, ebenfalls Druck auf ihren jeweiligen Gegenüber auszuüben. In ihrem Falle ist jedoch eine zumindest offizielle Distanz zu den Proxy-Akteuren im Sinne der *plausible deniability* noch wichtiger, um die angestrebte Machtfunktion auch erfüllen zu können. Die Debatte um die weltweite Involvierung des chinesischen Technikunternehmens Huawei am Ausbau nationaler 5G-Netze demonstriert dabei Huawei’s Bedeutung als Machtressource, sowie die steigende Bedrohungsperzeption des Unternehmens seitens demokratischer Staaten. Allen voran die USA sehen in Huawei in erster Linie einen staatlichen Proxy der chinesischen Regierung, um auch im digitalen Bereich, ähnlich wie die neue Seidenstraßeninitiative im Offline-Bereich, die eigenen Hardpower-Ressourcen auf digitaler Ebene noch stärker auszubauen (Demchak 2019, S. 102). Dass die chinesische Führung Huaweis Hardpowerfunktionen, im Sinne der Kontrolle weltweiter 5G-Netzwerke als bedeutender einstuft als die Softpowerfunktionen von Unternehmen wie Alibaba oder Tencent, die stärker im Bereich der Unterhaltung und des „Lifestyle“-Sektors aktiv sind, indiziert zumindest das zuletzt repressive Vorgehen der Regierung gegen deren Expansionspläne im Bereich der Finanz-Technologie (Smith 2021).

Proxies sind somit nicht nur staatliche Machtressourcen auf internationaler Ebene, sondern können auch selbst Gegenstand staatlicher Machtverteilungskonflikte werden. Die Debatte um staatliche Sorgfaltspflichten (*Due Diligence*) gegenüber dem Handeln ihrer Bürger im digitalen Raum zeigt dabei auf, dass insbesondere autokratische Regierungen eine gewisse Machtlosigkeit gegenüber dem Handeln nationaler Akteure vorgeben, um deren Machtfunktionen weiterhin effektiv im Sinne der eigenen Verantwortlichkeitsverschleierung nutzen zu können. Es mag zwar vielleicht sogar in vielen Fällen stimmen, dass Akteure wie patriotische Hacker selbst initiativ geworden sind, bzw. keine materielle Unterstützung seitens staatlicher Stellen erhalten haben. Dennoch wird ideologische Unterstützung als autokratische Softpower-Ressource, bzw. die alleinige Kenntnis über bevorstehende Cyberoperationen oftmals bereits im Spektrum staatlicher Verantwortlichkeit für Cyberoperationen nationaler Akteure angesiedelt (Healey 2011, S. 60).

Aufgrund der dezentralen und entterritorialisierten Grundstruktur des Internets betrifft Macht im Cyberspace noch sehr viel stärker die internationale Umwelt der jeweiligen Akteure, im Vergleich zur analogen Ebene. Dies führte jedoch in den letzten Jahren dazu, dass nicht nur autokratische Regime vermehrt Kontrolle über

die *Fifth Domain* zu erreichen versuchen. Auch demokratische Staaten, wie etwa die USA unter Donald Trump mit ihrer *„Clean Networks Initiative"*, verfolgten bislang zumindest zeitweise eine Art „Techno-Nationalismus", um größere Kontrolle über Hardpower-Ressourcen des Cyberspace zu erlangen. Private Unternehmen sowie zivilgesellschaftliche Akteure fungieren dabei für beide Regimetypen zeitweise als Proxies, vor allem im Hinblick auf die Prägung des internationalen Diskurses durch Softpower-Funktionen. Dies gereicht den jeweiligen Regierungen jedoch nur so lange zum Vorteil, wie sich die stets hinreichend autonom agierenden Akteure auch mit der angestrebten Machtfunktion identifizieren können, bzw. in deren Sinne handeln.[18]

7 Schlussfolgerungen

Der vorliegende Bericht hat aufgezeigt, dass der theoretische Zugang zu Macht im digitalen Raum noch komplexer erfolgen muss als im Falle der analogen Sphäre. Aufgrund nach wie vor noch nicht ausreichender Grundlagenforschung im Hinblick auf Ursache-Wirkungszusammenhänge bezüglich offensiver Cyberoperationen, defizitärer völkerrechtlicher Regulierungsversuche, sowie der dezentralen, entgrenzten Funktionslogik des Mediums an sich, erscheint die Verteilung und Ausgestaltung von Machtpotenzialen zwischen unterschiedlichen Akteuren im Cyberspace oftmals als ein kontextspezifischer Aushandlungsprozess. Anhand des Konzepts des Proxys wird dies besonders deutlich: Unterschiedliche Akteure können dabei zur Machtressource für primär, jedoch nicht ausschließlich staatliche Bestrebungen werden, die eigene Machtposition im digitalen Raum zu behaupten, oder gar auszuweiten. Der Vergleich zwischen offensiven und defensiven Cyberproxies machte dabei die Komplexität verschiedenster Proxy-Tätigkeiten im Rahmen unterschiedlicher Machtfunktionen deutlich. Das bislang oftmals als weitestgehend moderat beschriebene Cyberkonfliktniveau kann dabei etwa als äquifinales Resultat des gleichzeitigen Wirkens offensiver, sowie defensiver Cyberproxy-Strategien autokratischer sowie demokratischer Staaten erklärt werden (Lindsay 2015).

Der in gewisser Weise voneinander abhängige Einsatz offensiver und defensiver Cyberproxies im Rahmen von Cyberkonflikten zeigt zudem auf, welche Herausforderungen sich staatlichen Akteuren durch Interaktionen im digitalen Raum stellen, jedoch auch, welche Flexibilität ihnen das Konfliktaustragungsmedium im Hinblick auf unterschiedliche Machtressourcen, -funktionen und -ebenen liefert (vgl. Borghard und Lonergan 2019, S. 129).

Grundlegend fokussiert sich Macht im Cyberspace noch sehr viel stärker auf Informationen als zentrale Ressource. Zwar können durch Cyberoperationen auch physische Effekte erzielt werden, jedoch besitzen selbst in einem solchen Fall die

[18] Das Beispiel des Ende 2020 zeitweise sogar verschwundenen Alibaba-Gründers Jack Ma verdeutlicht dabei, dass auch im autoritären China global agierende Unternehmen mit der Zeit Eigeninteressen entwickeln und verfolgen können, die teilweise denen des Regimes zuwiderlaufen (Cheung und Wilhelm 2021). Jedoch verfügen Autokratien zumeist über umfangreichere, auf Zwang basierende Hardpower-Ressourcen, um die Macht dieser Akteure nicht zu groß, bzw. zu einer Gefahr für das eigene Regime werden zu lassen.

Akteure der Opferseite diverse Möglichkeiten, eigene Machtressourcen zum Einsatz zu bringen, um die gegnerische Machtentfaltung auf der Hardpower-Ebene zu reduzieren. Dies kann wie beschrieben durch Geheimhaltungs-, bzw. Verschleierungstaktiken im Rahmen öffentlicher Attributionsprozesse, jedoch auch durch die Erweiterung defensiver Machtpotenziale im Rahmen von PPPs erfolgen. Hinzu kommt, dass selbst der Einsatz von Hardpower-Funktionen mit Hilfe von ISPs oftmals auf die physische Einschränkung des Zugangs ziviler Akteure zu Kommunikationskanälen und somit zu Informationen als bedeutender Softpower-Ressource ausgerichtet ist. Die bloße Zerstörung durch Zwang als zentrale Machtfunktion widerspricht der Logik des Cyberspace, bzw. können dessen Machtressourcen für eine derartige Machtfunktion im Vergleich zu analogen Mitteln als weitaus ineffizienter angesehen werden. Hieran knüpft beispielsweise auch die Debatte um das Konzept des „Cyberterrorismus“ an, da der Terror-Begriff auf der Kreierung und Verbreitung von Macht durch Gewalt basiert, was gleichermaßen auf analoger Ebene nach wie vor effektiver und effizienter zu erreichen sein dürfte als im Cyberspace.

Nichtsdestotrotz zeitigen auch informationsbasierte Machtfunktionen im Cyberspace *Spillover*-Effekte für analoge Konflikte: Etwa durch die Manipulation der Kriegsberichtserstattung, oder auch durch polarisierende Wirkweisen offensiver Proxyoperationen gegenüber ausländischen Bevölkerungen, zur Ausnutzung/Vertiefung bereits bestehender Konfliktlinien auf domestischer Ebene. Zudem geraten die Eskalationspotenziale von Cyberoperationen auf Nuklearwaffen-Systeme vermehrt in den wissenschaftlichen Fokus, wobei ebenfalls hierdurch entstehende oder verschärfte Informationsasymmetrien im Rahmen des Abschreckungskomplexes als potenziell konfliktverschärfend ausgemacht werden (z. B. MacDonald 2020). Für die Zukunft ebenfalls zunehmend bedeutend könnte zudem die Instrumentalisierung bestimmter Bestandteile der globalen Internetinfrastruktur, wie dem Border Gateway Protocol, seitens autokratischer Regime wie dem Iran sein (vgl. Salamatian et al. 2021).

Die bis hierhin noch nicht erwähnte Debatte um mögliche Cyberwaffenkontrollregime verdeutlicht ebenfalls die Bedeutung situativer Aspekte für eine Analyse von Macht im Cyberspace (Liff 2012; Hansel et al. 2018; Stevens 2018): Ob und wann verschiedene Akteure oder auch technische Werkzeuge zu offensiven oder defensiven Machtressourcen werden, hängt in erster Linie vom jeweiligen Kontext, bzw. der Motivation des Akteurs ab. Gleiches gilt auch für nichtstaatliche Akteure, welche in unterschiedlichen Proxy-Rollen agieren können. So implizieren die Hacking-Fähigkeiten privater Akteure nicht zwingend eine konfliktive Dimension. Dies ist erst der Fall, sobald sie diese eigeninitiativ oder auf Anleitung staatlicher (oder auch nichtstaatlicher) Auftraggeber mit einem schädigenden Ziel einsetzen. Gleichzeitig beweist der Fall der 2016 abhanden gekommenen NSA-Sicherheitslücken, dass selbst für staatliche Akteure wie die USA die Kontrolle über die eigenen Machtressourcen im Cyberspace ungleich schwerer zu behaupten ist als im Falle konventioneller Konfliktaustragungsmittel.

Künftige Forschungsvorhaben sollten sich demnach (noch stärker) besonders folgenden Aspekten widmen, um die multidimensionale Wirkweise varianter Machtressourcen im digitalen Raum noch genauer erfassen zu können:

1. Dem Zusammenspiel diskursiver Machtfunktionen auf der Softpower-Ebene, zur Stärkung eigener, oder Einhegung fremder Hardpower-Ressourcen, mit einem Fokus auf Regimetypenunterschiede und somit auch der Frage, wie durch Diskursmacht Desinformation analytisch greifbar gemacht werden kann, 2. den demokratietheoretischen Auswirkungen der autokratischen Integration informationsbasierter Machtfunktionen offensiver Cyberproxies, sowie 3. der Salienz autonomer Machtpotenziale nichtstaatlicher Akteure, im Kontext sich wiederholender Staat-Proxy-Beziehungsformen. Letzteres könnte sich etwa auch auf erweiterte, mit dem Cyberspace verbundene Sphären, wie etwa den Weltraum beziehen: Hier scheint sich eine Verschiebung der Machtverhältnisse anzudeuten, indem private Unternehmen zunehmend das satellitengestützte Informationsmonopol staatlicher Akteure aufbrechen (Lin-Greenberg und Milonopoulos 2021).

Danksagung Der vorliegende Beitrag entstand im Rahmen des von der Deutschen Stiftung Friedensforschung geförderten Forschungsprojektes „Sicherheit durch Verschleierung: Warum Regierungen Proxies in Cyberkonflikten einsetzen“.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Allagui, Ilhem, und Johanne Kuebler. 2011. The Arab Spring and the role of ICTs. *International Journal of Communication* 5:8.

Amnesty International. 2021. Out of control: failing EU laws for digital surveillance export. Amnesty international. https://www.amnesty.org/download/Documents/ EUR0125562020ENGLISH.PDF. Zugegriffen: 29. Jan. 2021.

Anderson, Collin, und Karim Sadjadpour. 2018. *Iran's Cyber threat: espionage, sabotage, and revenge*. Washington, D.C.: Carnegie Endowment for International Peace.

Baram, Gil, und Udi Sommer. 2019. Covert or not covert: national strategies during cyber conflicts. In *11th international conference on Cyber conflict: silent battle*, Hrsg. T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, und G. Visky, 197–212. Tallinn: NATO CCD COE Publications.

Barlow, John Perry. 1996. A declaration of the independence of cyberspace. Electronic frontier foundation. https://www.eff.org/cyberspace-independence. Zugegriffen: 9. Juni 2020.

Barnett, Michael, und Raymond Duvall. 2005. Power in international politics. *International Organization* 59(01):39–75. https://doi.org/10.1017/S0020818305050010.

Bendiek, Annegret, und Andrew L. Porter. 2013. European Cyber Security Policy within a Global Multistakeholder Structure. *European Foreign Affairs Review* 18(2):155–180.

Berman, Eli, und David A. Lake. 2019. *Proxy wars: suppressing violence through local agents*. Ithaca: Cornell University Press.

Blackberry. 2020. BAHAMUT: hack-for-hire masters of phishing, fake news, and fake apps. Blackberry. https://www.blackberry.com/us/en/forms/enterprise/bahamut-report. Zugegriffen: 30. Jan. 2021.
Blank, Stephen. 2017. *Cyber and Information War à la Russe. In Understanding cyber conflict: 14 analogies*., 81–98. Washington, D.C.: Georgetown University Press.
Boeke, Sergei, und Dennis Broeders. 2018. The demilitarisation of cyber conflict. *Survival* 606:73–90. https://doi.org/10.1080/00396338.2018.1542804.
Borghard, Erica D., und Shawn W. Lonergan. 2016. Can states calculate the risks of using cyber proxies? *Orbis* 603:395–416. https://doi.org/10.1016/j.orbis.2016.05.009.
Borghard, Erica D., und Shawn W. Lonergan. 2017. The logic of coercion in cyberspace. *Security Studies* 263:452–481. https://doi.org/10.1080/09636412.2017.1306396.
Borghard, Erica D., und Shawn W. Lonergan. 2019. Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly* 133:122–145.
Boulding, Kenneth E. 1990. *Three faces of power*. London: SAGE.
Bronk, Christopher, und Eneken Tikk-Ringas. 2013. The cyber-attack on Saudi Aramco. *Survival* 552:81–96.
Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, und Nacho Díaz-Castaño. 2020. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies* https://doi.org/10.1080/14616696.2020.1804973.
Canfil, Justin Key. 2016. Honing cyber attribution. The cyber issue. *Journal of International Affairs* 70(1):217–226.
Carr, Jeffrey. 2011. *Inside cyber warfare: Mapping the cyber underworld*, 2. Aufl., Sebastopol: O'Reilly & Associates.
Carr, Madeline. 2016. Public-private partnerships in national cyber-security strategies. *International Affairs* 92(1):43–62. https://doi.org/10.1111/1468-2346.12504.
Cheung, Rachel, und Benjamin Wilhelm. 2021. Is Beijing about to make an example out of Jack ma? World politics review. https://www.worldpoliticsreview.com/trend-lines/29353/is-beijing-about-to-make-an-example-out-of-jack-ma. Zugegriffen: 30. Jan. 2021.
Christensen, Kristoffer Kjærgaard, und Karen Lund Petersen. 2017. Public–private partnerships on cyber security: a practice of loyalty. *International Affairs* 936:1435–1452. https://doi.org/10.1093/ia/iix189.
Collier, Jamie. 2017. Proxy actors in the cyber domain: Implications for state strategy. *St Antony's International Review* 13(1):25–47.
Connell, Michael, und Sarah Vogler. 2017. Russia's Approach to Cyber Warfare. CNA. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf. Zugegriffen: 10. Juni 2020.
Deibert, Ronald J. 2009. *The geopolitics of internet control: censorship, sovereignty, and cyberspace*. Routledge handbook of internet politics., 323–336.
Deibert, Ronald J., Rafal Rohozinski, und Masashi Crete-Nishihata. 2012. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security dialogue* 43(1):3–24. https://doi.org/10.1177/0967010611431079.
Demchak, Chris C. 2019. China: determined to dominate cyberspace and AI. *Bulletin of the Atomic Scientists* 753:99–104. https://doi.org/10.1080/00963402.2019.1604857.
Do, J. 2020a. Seven international Cyber defendants, including "apt41" actors, charged in connection with computer intrusion campaigns against more than 100 victims globally. Department of justice. https://www.justice.gov/opa/press-release/file/1317206/download. Zugegriffen: 1. Juli 2021.
Do, J. 2020b. Two Chinese hackers working with the ministry of state security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research. US department of justice. https://www.justice.gov/opa/press-release/file/1295981/download. Zugegriffen: 25. Mai 2021.
Drezner, Daniel W., Henry Farrell, und Abraham L. Newman. 2021. *The uses and abuses of weaponized interdependence*. Washington, DC: Brookings Institution Press.
Egloff, Florian J. 2018. Cybersecurity and non-state actors: a historical analogy with mercantile companies, privateers, and pirates. https://ora.ox.ac.uk/objects/uuid:77eb9bad-ca00-48b3-abcf-d284c6d27571. Zugegriffen: 8. Juni 2020.
Egloff, Florian J. 2020. Public attribution of cyber intrusions. *Journal of Cybersecurity* 6(1):484. https://doi.org/10.1093/cybsec/tyaa012.
Egloff, Florian J., und Max Smeets. 2021. Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies* https://doi.org/10.1080/01402390.2021.1895117.
Eichensehr, Kristen. 2017. Public-private cybersecurity. *Texas Law Review* 95:467–538.
Eichensehr, Kristen E. 2019. Decentralized cyberattack attribution. *AJIL Unbound* 113:213–217. https://doi.org/10.1017/aju.2019.33.

Finnemore, Martha, und Duncan B. Hollis. 2020. Beyond naming and shaming: accusations and international law in cybersecurity. *European Journal of International Law* https://doi.org/10.1093/ejil/chaa056.
Floyd, Garry S. 2018. Attribution and operational art: implications for competing in time. *Strategic Studies Quarterly* 122:17–55.
Gartzke, Erik. 2013. The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security* 382:41–73. https://doi.org/10.1162/ISEC_a_00136.
Gilli, Andrea, und Mauro Gilli. 2019. Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security* 433:141–189.
Gioe, David V. 2018. Cyber operations and useful fools: the approach of Russian hybrid intelligence. *Intelligence and National Security* 337:954–973. https://doi.org/10.1080/02684527.2018.1479345.
Göbel, Christian. 2012. Das Innovationsdilemma und die Konsolidierung autokratischer Regime (The Innovation Dilemma and the Consolidation of Autocratic Regimes). *Politische Vierteljahresschrift* 47:132–156.
Hansel, Mischa, Max Mutschler, und Marcel Dickow. 2018. Taming cyber warfare: lessons from preventive arms control. *Journal of Cyber Policy* 3(1):44–60. https://doi.org/10.1080/23738871.2018.1462394.
Hansen, Lene, und Helen Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly* 534:1155–1175.
Harnisch, Sebastian, und Kerstin Zettl. 2020. Blame Game im Cyberspace. Informationstechnik als Waffe? *Ruperto Carola* 12:96–105. https://doi.org/10.17885/heiup.ruca.2020.16.24194.
Harris, Shane. 2008. China's cyber-militia. *Nextgov*. https://www.nextgov.com/cio-briefing/2008/05/chinas-cyber-militia/42113/. Zugegriffen: 20. Juni 2021.
Hauben, Michael, und Ronda Hauben. 1998. Netizens: on the history and impact of usenet and the internet. *First Monday* https://doi.org/10.5210/fm.v3i7.605.
Healey, Jason. 2011. The spectrum of national responsibility for cyberattacks. *The Brown Journal of World Affairs* 18(1):57–70. http://www.jstor.org/stable/24590776.
Hinck, Garrett, und Tim Maurer. 2019. What's the point of charging foreign state-linked hackers? Lawfare. https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers. Zugegriffen: 29. Jan. 2021.
Hurel, Louise Marie, und Luisa Cruz Lobato. 2018. Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy* 3(1):61–76. https://doi.org/10.1080/23738871.2018.1467942.
IISS. 2021. Cyber capabilities and national power: a net assessment. International institute for strategic studies. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power. Zugegriffen: 19. Aug. 2021.
Inglis, Chris. 2019. Illuminating a new domain: the role and nature of military intelligence, surveillance and reconnaissance in cyberspace. In *Bytes, bombs, and spies: the strategic dimensions of offensive cyber operations*, Hrsg. Herbert Lin, Amy B. Zegart, 19–45. Washington, D.C.: Brookings Institution Press.
Insikt Group. 2017. North Korea's ruling elite are not isolated. Recorded Future. https://www.recordedfuture.com/north-korea-internet-activity/. Zugegriffen: 8. Juni 2020.
Jensen, Eric Talbot, und Sean Watts. 2017. A cyber duty of due diligence: gentle civilizer or crude destabilizer. *Texas Law Review* 95:1555–1577.
Jensen, Benjamin, Brandon Valeriano, und Ryan Maness. 2019. Fancy bears and digital trolls: cyber strategy with a Russian twist. *Journal of Strategic Studies* 422:212–234. https://doi.org/10.1080/01402390.2018.1559152.
Kaspersky. 2020. DeathStalker: detailed look at a mercenary APT group that spies on small and medium businesses. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_deathstalker-detailed-look-at-a-mercenary-apt-group-that-spies-on-small-and-medium-businesses. Zugegriffen: 27. Jan. 2021.
Kendall-Taylor, Andrea, Erica Frantz, und Joseph Wright. 2020. The digital dictators: how technology strengthens autocracy. *Foreign Affairs* 99:103.
Keohane, Robert O. 1984. *After hegemony: cooperation and discord in the world political economy*. Princeton, Oxford: Princeton University Press.
King, Gary, Jennifer Pan, und Margaret E. Roberts. 2013. How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 1072:326–343.
Kirsch, Cassandra. 2014. The Grey hat hacker: reconciling cyberspace reality and the law. *Northern Kentucky Law Review* 413:383–404.
Klimburg, Alexander. 2010. The whole of nation of cyberpower. *Georgetown Journal of International Affairs* 11:171.

Klimburg, Alexander. 2011. Mobilising cyber power. *Survival* 53(1):41–60. https://doi.org/10.1080/00396338.2011.555595.
Kostyuk, Nadiya, und Yuri M. Zhukov. 2019. Invisible digital front: can cyber attacks shape battlefield events? *Journal of Conflict Resolution* 632:317–347. https://doi.org/10.1177/0022002717737138.
Kwon, Bo Ram. 2016. The conditions for sanctions success: a comparison of the Iranian and North Korean cases. *Korean Journal of Defense Analysis* 28(1):139–161.
Ladwig, Walter C., III. 2008. A cold start for hot wars? The Indian army's new limited war doctrine. *International Security* 323:158–190.
Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. Santa Monica: RAND Corporation.
Libicki, Martin C. 2018. Expectations of cyber deterrence. *Strategic Studies Quarterly* 124:44–57.
Liff, Adam P. 2012. Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies* 353:401–428. https://doi.org/10.1080/01402390.2012.663252.
Lin, Herbert. 2019. The existential threat from cyber-enabled information warfare. *Bulletin of the Atomic Scientists* 754:187–196.
Lin-Greenberg, Erik, und Theo Milonopoulos. 2021. Private eyes in the Sky: emerging technology and the political consequences of eroding government secrecy. *Journal of Conflict Resolution* https://doi.org/10.1177/0022002720987285.
Lindsay, Jon R. 2015. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity* 1(1):53–67. https://doi.org/10.1093/cybsec/tyv003.
Liu Yuying, Ian. 2017. State responsibility and cyberattacks: Defining due diligence obligations. *Indonesian Journal of International & Comparative Law* 42:191–259.
Long, Tom. 2017. It's not the size, it's the relationship: from ‚small states' to asymmetry. *International Politics* 542:144–160. https://doi.org/10.1057/s41311-017-0028-x.
Lutscher, Philipp M., Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, und Alberto Dainotti. 2020. At home and abroad: the use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution* 642(3):373–401. https://doi.org/10.1177/0022002719861676.
Lyngaas, Sean. 2021. Alleged North Korean hackers scouted crypto exchange employees before stealing currency, researchers say. Cyberscoop. https://www.cyberscoop.com/north-korea-lazarus-group-cryptocurrency-exchanges/. Zugegriffen: 10. Aug. 2021.
MacDonald, Bruce W. 2020. Growing stability challenges to the nuclear weapons domain. *SAIS Review of International Affairs* 40(1):125–137. https://doi.org/10.1353/sais.2020.0011.
Malley, Robert. 2019. 10 conflicts to watch in 2020. Foreign policy. https://foreignpolicy.com/2019/12/26/10-conflicts-to-watch-2020/. Zugegriffen: 10. Juni 2020.
Maness, Ryan C., und Brandon Valeriano. 2016. The impact of cyber conflict on international interactions. *Armed Forces & Society* 422:301–323. https://doi.org/10.1177/0095327X15572997.
Maoz, Zeev, und Belgin Şan-Akca. 2012. Rivalry and state support of non-state armed groups (NAGs), 1946–2001. *International Studies Quaterly* 564:720–734. https://doi.org/10.1111/j.1468-2478.2012.00759.x.
Maurer, Tim. 2016. Proxies' and cyberspace. *Journal of Conflict and Security Law* 213:383–403. https://doi.org/10.1093/jcsl/krw015.
Maurer, Tim. 2018a. *Cyber mercenaries*. Cambridge: Cambridge University Press.
Maurer, Tim. 2018b. Cyber proxies and their implications for liberal democracies. *The Washington Quarterly* 412:171–188. https://doi.org/10.1080/0163660X.2018.1485332.
Maurer, Tim, und Kenneth Geers. 2015. Cyber proxies and the crisis in Ukraine. In *Cyber war in perspective: Russian aggression against Ukraine*, Hrsg. Kenneth Geers, 79–86. Tallinn: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.
Moghadam, Assaf, und Michel Wyss. 2020. The political power of proxies: why nonstate actors use local surrogates. *International Security* 444:119–157. https://doi.org/10.1162/ISEC_a_00377.
Mueller, Milton L. 2020. Against sovereignty in cyberspace. *International Studies Review* 224:779–801.
Mueller, Milton, Karl Grindal, Brenden Kuerbis, und Farzaneh Badiei. 2019. Cyber attribution: can a new institution achieve transnational credibility? *The Cyber Defense Review* 4(1):107–122.
Mumford, Andrew. 2013. *Proxy warfare*. Hoboken: Wiley.
Nye, Joseph S. 1990. Soft power. *Foreign Policy* 80:153–171.
Nye, Joseph S. 2002. *The paradox of American power: why the world's only superpower can't go it alone*. Oxford: Oxford University Press.
Nye, Joseph S. 2010. *Cyber power*. Harvard: Harvard Kennedy School.

Nye, Joseph S. 2018. Protecting democracy in an era of cyber information war. Hoover institution. https://www.hoover.org/research/protecting-democracy-era-cyber-information-war. Zugegriffen: 12. Mai 2020.
Ottis, Rain. 2011. Theoretical offensive cyber militia models. *Leading Issues in Information Warfare and Security Research* 1:307–313.
Palmer, Charles C. 2001. Ethical hacking. *IBM Systems Journal* 403:769–780.
Pierskalla, Jan H., und Florian M. Hollenbach. 2013. Technology and collective action: The effect of cell phone coverage on political violence in Africa. *American Political Science Review* 107(2):207–224.
Pinkston, Daniel A. 2020. North korea's objectives and activities in cyberspace. *Asia Policy* 272:76–83.
Poznansky, Michael, und Evan Perkoski. 2018. Rethinking secrecy in cyberspace: the politics of voluntary attribution. *Journal of Global Security Studies* 34:402–416.
Raud, Mikk. 2015. China and cyber: attitude, strategies, organisation. NATO CCD COE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf. Zugegriffen: 10. Jan. 2021.
Rivera, Jason. 2015. Achieving cyberdeterrence and the ability of small states to hold large states at risk. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon)*. Tallinn, 26–29 May 2015., Hrsg. M. Maybaum, 7–24. Piscataway: IEEE.
Rød Geelmuyden, Espen, und Nils B. Weidmann. 2015. Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research* 523:338–351.
Roguski, Przemysław. 2020. Application of International Law to cyber operations: a comparative analysis of States' views. https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y. Zugegriffen: 11. Juni 2020.
Romanosky, Sasha. 2017. Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government? Lawfare. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government. Zugegriffen: 13. Juli 2020.
Roose, Kevin. 2021. In pulling trump's megaphone, twitter shows where power now lies. The New York Times. https://www.nytimes.com/2021/01/09/technology/trump-twitter-ban.html. Zugegriffen: 25. Jan. 2021.
Salamatian, Loqman, Frédérick Douzet, Kavé Salamatian, und Kévin Limonier. 2021. The geopolitics behind the routes data travel: a case study of Iran. *Journal of Cybersecurity* 7(1):1–19. https://doi.org/10.1093/cybsec/tyab018.
Sanger, David E. 2021. Revil, hacking group behind major Ransomware attack, disappears. The New York Times. https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html. Zugegriffen: 10. Aug. 2021.
Schmitt, Michael N., und Liis Vihul. 2014. Proxy wars in cyberspace: the evolving international law of attribution. *Fletcher Security Review* 1:53.
Schörnig, Niklas, und Alexander C. Lembcke. 2006. The vision of war without casualties: On the use of casualty aversion in armament advertisements. *Journal of Conflict Resolution* 502:204–227.
Schulze, Matthias. 2020. Cyber in war: assessing the strategic, tactical, and operational utility of military cyber operations. In *12th international conference on cyber conflict 20/20 vision: the next decade*, Hrsg. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, und G. Visky, 183–197.
Shires, James. 2019. Hack-and-leak operations: intrusion and influence in the Gulf. *Journal of Cyber Policy* 42:235–256. https://doi.org/10.1080/23738871.2019.1636108.
Shires, James, und Michael McGetrick. 2021. *Rational Not Reactive: Re-evaluating Iranian Cyber Strategy*. Harvard Kennedy School, Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/311328%20Belfer_V4.pdf. Zugegriffen: 8. Okt. 2021.
Smith, Noah. 2021. Why is China smashing its tech industry? Noahpinion. https://noahpinion.substack.com/p/why-is-china-smashing-its-tech-industry?token=eyJ1c2VyX2lkIjozMTU4OSwicG9zdF9pZCI6MzkxNjg0MDcsIl8iOiJxUEx3dSIsImlhdCI6MTYyNzQxNDM0NywiZXhwIjoxNjI3NDE3OTQ3LCJpc3MiOiJwdWItMzUzNDUiLCJzdWIiOiJwb3N0LXJlYWN0aW9uIn0.32h. Zugegriffen: 4. Aug. 2021.
Steffens, Timo. 2018. *Auf der Spur der Hacker: Wie man die Täter hinter der Computer-Spionage enttarnt*. Berlin: Springer Vieweg.
Stevens, Tim. 2018. Cyberweapons: power and the governance of the invisible. *International Politics* 553:482–502.
Strickling, Lawrence E., und Jonah Force Hill. 2017. Multi-stakeholder internet governance: successes and opportunities. *Journal of Cyber Policy* 23:296–317. https://doi.org/10.1080/23738871.2017.1404619.

Tsagourias, Nicholas. 2012. Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law* 172:229–244. https://doi.org/10.1093/jcsl/krs019.

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

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, und Anna Schwarzenbach. 2020. National Cyber power index 2020: methodology and analytical considerations. Harvard kennedy school, belfer center for science and international affairs. https://www.belfercenter.org/publication/national-cyber-power-index-2020#:~:text=The%20Belfer%20National%20Cyber%20Power, collected%20from%20publicly%20available%20data.. Zugegriffen: 25. Jan. 2021.

Warren, Matthew, und Shona Leitch. 2016. The Syrian Electronic Army—a hacktivist group. *Journal of Information, Communication and Ethics in Society* 142:200–212. https://doi.org/10.1108/JICES-12-2015-0042.

Weber, Max. 1972. *Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie*, 5. Aufl., Tübingen: Mohr Siebeck.

Williams, Brad D. 2021. Proposed ‚hack-back' bill tells DHS to study allowing companies to retaliate. Breaking defense. https://breakingdefense.com/2021/07/proposed-hack-back-bill-tells-dhs-to-study-allowing-companies-to-retaliate/. Zugegriffen: 10. Aug. 2021.

Wolff, Josephine. 2021. What if the best defense is a good defense (instead of offense Rebranded as active defense)? Offensive cyber working group. https://offensivecyber.org/2021/08/18/what-if-the-best-defense-is-a-good-defense-instead-of-offense-rebranded-as-active-defense/. Zugegriffen: 19. Aug. 2021.

Womack, Brantly. 2016. *Asymmetry and international relationships*. Cambridge: Cambridge University Press.

Zeitzoff, Thomas. 2017. How social media is changing conflict. *Journal of Conflict Resolution* 619: 1970–1991.

Zettl, Kerstin. 2020. Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland. *Zeitschrift für Außen- und Sicherheitspolitik* 12:429–451. https://doi.org/10.1007/s12399-020-00789-7.