1. Einleitung: Die Übertragung der Staat-Proxy-Logik auf den Cyberspace

Australischer Verteidigungsminister: »Is this China?«
Chef des Australischen Geheimdiensts (ASD): »A viable possibility, we can't discount al Qaeda, North Korea…«
Australische Justizministerin: »Speculation is no help.«
Chef des Australischen Geheimdiensts (ASD): »It could be homegrown. Though they haven't tripped alerts. We have had no warning.«
Australischer Verteidigungsminister:
»For christ's sake people, we know who it is!«.
Transkription aus der Streaming-Serie »Secret City«, Staffel 1, Folge 4

1.1 Autokratien und Demokratien: unterschiedliche Proxy-Nutzung im Cyberspace?

Der hier vorgestellte Dialog entstammt zwar einer fiktiven Serie, könnte sich jedoch so oder in ähnlicher Form auch in der Realität in einem nationalen ›Situation-Room‹ abspielen. In der Serienepisode hatten unbekannte Hacker das Flugkommunikationssystem Australiens und somit Teile der kritischen Infrastrukturen des Landes unter ihre Kontrolle gebracht. Wie der Dialog verdeutlicht, vermuteten die Verantwortlichen zwar einen politischen Rivalen, konkret die Volksrepublik (VR) China, als Urheber, konnten dies jedoch noch nicht mit entsprechenden Beweisen belegen. Gleichzeitig verwies der Geheimdienstchef auf die Möglichkeit alternativer Attributionen in Richtung nichtstaatlicher AkteurInnen. Die Frage der Attribution erlangte in den letzten zehn Jahren Bedeutung im öffentlichen, politischen sowie wissenschaftlichen Diskurs über Cyberkonflikte. Verstärkt wird das dabei thematisierte ›Attributionsproblem‹ nicht nur durch die

bereits bestehenden technischen Herausforderungen des dezentralen Internets als Konfliktaustragungsraum, sondern auch durch den Einsatz von StellvertreterInnen für die Durchführung offensiver Cyberoperationen. In der Geschichte dienten nichtstaatliche AkteurInnen Staaten im Rahmen traditioneller Konflikte bereits in vielen Fällen als nützliche Partner, Erfüllungsgehilfen oder auch Sündenböcke. Gerade zu Zeiten des Kalten Krieges kam es sowohl auf Seiten der USA als auch der Sowjetunion (UdSSR) zur unterschiedlichen Instrumentalisierung dieser *Proxys* im Rahmen der sog. ›Stellvertreterkriege‹. Dabei unterstützten die USA etwa die Contra-Rebellen in Nicaragua (Klare 1989), die UdSSR sponserten die Palästinensische Befreiungsorganisation (PLO) (Spiegel 1983, S. 51). Somit mischten sich die beiden Großmächte in bereits bestehende Konflikte außerhalb ihres Staatsgebietes ein, indem sie eine der nationalen Konfliktparteien materiell und/oder immateriell unterstützten. Durch diese Form der ›indirekten Intervention‹ (Mumford 2013) konnten die Staaten ihre Interessen im Rahmen der Konflikte verfolgen, ohne dabei zu direkten Konfliktparteien zu werden und entsprechende politische und ökonomische Kosten tragen zu müssen. Da sowohl der unterstützende Staat als auch der Proxy ihre bestehende Beziehung öffentlich nicht eingestehen, gelingt es insbesondere dem staatlichen ›Benefactor‹ (Wohltäter/Sponsor), die sog. ›Plausible Deniability‹ (plausible Bestreitbarkeit) über die eigene Involvierung in den Konflikt zu bewahren. Außer aufgrund der reinen Kostenersparnis sowie einer niedrigeren Eskalationsgefahr lohnte sich eine Unterstützung einheimischer KonfliktakteurInnen aus Sicht der Staaten ferner, da diese über einen ›Local Advantage‹ im Konfliktaustrag verfügten, z.B. die geografischen Gegebenheiten des Landes besser kannten, als dies den eigenen Militärtruppen im Rahmen einer direkten Intervention hätte möglich sein können (vgl. Mumford 2013).

In der neueren Historie der wissenschaftlichen und öffentlichen Verwendung des Proxy-Begriffes wird diesem immer häufiger das Präfix ›Cyber‹ vorangestellt. Eine Google-(Scholar)-Suche des Begriffes *Cyberproxy* fördert dabei jedoch im Gegensatz zu den für die USA nachgewiesenen Beziehungen zu konventionellen Proxys fast ausschließlich Berichterstattungen über autokratische Stellvertreternutzungen im Cyberspace zu Tage. Wie lässt sich dieser Befund erklären? Sind Demokratien im Cyberspace schlicht nicht auf die Hilfe privater AkteurInnen zur Durchführung offensiver Operationen angewiesen oder verzichten sie gar regelmäßig auf eigene Cyberangriffe? Um die These demokratischer Zurückhaltung im Cyberspace in einem ersten Schritt zu testen, wird in dieser Arbeit im Zuge der empirischen Analyse auf einen umfassenden Cyberkonfliktdatensatz zurückgegriffen. Der Vergleich zwischen autokratischem und demokratischem Cyberkonfliktaustrag stellt jedoch nur eine notwendige Vorstufe dar, um die im Zentrum der Arbeit stehenden Proxys im Cyberspace regimetypenspezifisch untersuchen zu können. Dabei soll die Frage beantwortet werden, ob nichtstaatliche AkteurInnen auch für Demokratien im Cyberspace als Proxys fungieren können, jedoch nicht in der Rolle des Angreifers, sondern des Opfers von Cyberoperationen. Die zentralen Forschungsfragen lauten somit:

Welche Arten von Proxys im Cyberspace nutzen Autokratien und Demokratien trotz eigener, technischer Kapazitäten? Welche Funktionen übernehmen diese und unter welchen Bedingungen?

Bearbeitet werden diese Fragen aus der Perspektive des neuen Liberalismus nach Andrew Moravcsik: Zum einen erlaubt der liberale Theorieansatz die Inklusion nichtstaatlicher AkteurInnen auf beiden Seiten der Konfliktdyade, zum anderen kann durch

das Theoriemodell Moravcsiks der Einfluss von Präferenzordnungen auf unterschiedlichen Ebenen untersucht werden. So könnte eine ausschließliche Fokussierung auf sicherheitspolitische oder wirtschaftliche Präferenzen der Staaten die große Varianz der Interessen, die durch den Einsatz unterschiedlicher Proxys im Rahmen unterschiedlicher Cyberoperationen verfolgt werden sollen, nicht adäquat erfassen.

Ein Blick in die öffentliche Berichterstattung im Rahmen von Cyberoperationen[1] liefert für eine stärker defensiv geprägte Staat-Proxy-Beziehung auf demokratischer Seite erste Indizien: So dominieren vor allem private IT-Unternehmen den Detektions- und Attributionsdiskurs im Rahmen von Cyberoperationen, wie auch die spätere Analyse zeigen wird. Privatwirtschaftliche AkteurInnen decken Cyberoperationen zwischen Staaten und deren Proxys, jedoch auch nichtstaatlichen AkteurInnen, nicht nur häufig auf, sondern attribuieren diese zudem auch in immer mehr Fällen, oftmals in Richtung staatlicher UrheberInnen (vgl. Romanosky und Boudreaux 2021). Aus dieser Beobachtung wird in der Arbeit das Argument entwickelt, dass diese stellvertretende Attribution als defensive Funktion demokratischer IT-Unternehmen als Proxys im Rahmen von Cyberkonflikten gewertet werden sollte, im Gegensatz zu den offensiven Cyberoperationen autokratischer StellvertreterInnen.

Aus liberaler Theorieperspektive werden hierfür unterschiedliche Erklärungsansätze diskutiert und darauf aufbauend wird ein eigenes Erklärungsmodell entwickelt. Dieses soll es ermöglichen, nicht nur das empirische Puzzle bezüglich der Autokratie-Demokratie-Unterscheidung, sondern auch innerhalb der Lager zu beobachtende Varianzen hinsichtlich der offensiven (Hacking) oder defensiven (Attribution) Cyberproxynutzung erklären zu können. Die drei Spielarten des Liberalismus von Andrew Moravcsik dienen dabei als theoretische Erklärungsansätze, die es auf die Staat-Proxy-Beziehung im Cyberspace zu übertragen gilt. Dabei werden domestische Präferenzbildungsprozesse das Kernstück der Analyse darstellen, die den autokratischen und demokratischen Entscheidungsprozess auf außenpolitischer Ebene entscheidend prägen. Der unterschiedliche Herrschaftszugang bestimmter domestischer Gruppen dient als eine zentrale Erklärungsvariable für die überwiegend offensive vs. defensive Cyberproxynutzung der beiden Regimetypen.[2]

Mithilfe jeweils zweier Fallstudien (Russland und China sowie USA und Israel) werden Unterschiede der Cyberproxynutzung zwischen und innerhalb der beiden Regimetypenkategorien konzeptualisiert und aus liberaler Sicht erklärt.[3] Grundlage für die empirische Analyse der jeweiligen Cyberproxystrategien ist dabei ein umfassender Cyberkonfliktdatensatz (HD-CY.CON), der es erlaubt, im Gegensatz zu den bislang

1 Der Begriff ›Cyberoperationen‹ wird verwendet, um sowohl ›Cyber Network Exploitations‹, die vor allem Spionagetätigkeiten umfassen, als auch disruptivere Operationen, sog. ›Cyber Network Attacks‹, zu inkludieren (vgl. Lin 2010, S. 63).

2 Regime werden definiert als »*a set of rules that identifies: who has access to power; who is allowed to select the government; and under what conditions and limitations authority is exercised*« (Kailitz 2013, S. 39).

3 Ein »Fall« bedeutet im Rahmen dieser Arbeit die Cyberproxy-Nutzung eines Landes im Untersuchungszeitraum, entsprechend des theoretischen Verständnisses »*of a case to include many observations on the same variable*« (Levy 2008, S. 3).

vorherrschenden quantitativen Einzelfall- oder Small-N-Studien die theoretischen Annahmen auf einer möglichst breiten quantitativen Datenbasis überprüfen zu können.[4] Somit wird mit dieser Arbeit auch auf methodologischer Ebene ein Beitrag zur weitgehend noch in ihren Anfängen befindlichen Cyberkonfliktforschung geleistet, indem erstmals auf Grundlage einer umfassenden Datenbasis Large-N-Untersuchungen von Cyberoperationen angestellt und diese gleichzeitig im Rahmen eines Mixed-Methods-Designs auch für qualitative Analysemethoden nutzbar gemacht werden. Konzeptionell wird die Frage nach regimetypenspezifischen Charakteristika und deren Auswirkungen im vernetzten und interdependenten Konfliktaustragungsraum des Cyberspace erstmals direkt an staatliche Cyberkonfliktstrategien angebunden. Durch den liberalen Theorieansatz kann zudem zwischen stärker institutionell verorteten Aspekten der domestischen Interessensvertretung sowie deren tatsächlichen Inhalten auf unterschiedlichen Ebenen differenziert werden. Somit sollen auch potenzielle Gemeinsamkeiten unterschiedlicher Regimetypen aufgrund konvergierender Präferenzkonstellationen in einem Bereich identifiziert werden können. Insgesamt wird in der Arbeit jedoch von größeren Präferenzinkompatibilitäten zwischen Autokratien und Demokratien ausgegangen, was als zentrale Erklärung für die interdependente Proxy-Nutzung beider Regimetypen im Rahmen von Cyberoperationen angeführt wird.

Somit ergibt sich für die vorliegende Arbeit sowohl eine wissenschaftliche als auch eine gesellschaftliche Relevanz (vgl. King et al. 1994, S. 15): Zum einen wird durch die Entwicklung eines liberalen Erklärungsmodells unterschiedlicher Staat-Proxy-Beziehungen auf der Grundlage eines umfassenden Cyberkonfliktdatensatzes der Dialog zwischen Theorien und Daten über den aktuellen Forschungsstand hinaus vorangetrieben. Die Arbeit ist somit explorativ, da ein neuer Theorieansatz für ein noch untererforschtes Forschungsfeld entwickelt und empirisch getestet wird. Die Arbeit ist jedoch auch in Teilen theorietestend, da im Zuge des Schlusskapitels bereits bestehende Theorien als alternative Erklärungsansätze für die empirischen Befunde diskutiert werden sollen. Indem das Proxy-Modell auf hierfür bislang noch nicht prädestinierte AkteurInnen, die IT-Unternehmen demokratischer Länder, übertragen wird, erfolgt zudem die Dekontextualisierung eines bestehenden Theoriemodells. Dies geschieht sowohl hinsichtlich der Art der Handlungen, die seitens des Proxys stellvertretend für den Staat vorgenommen werden, als auch hinsichtlich des Konfliktaustragungsraumes. Bislang konzentrierte sich die politikwissenschaftliche Proxy-Forschung auf ›Proxy-Wars‹ im konventionellen Bereich und verortete Proxys somit stets als gewaltsame AkteurInnen im Rahmen militärischer Konflikte (vgl. Rauta 2021). Wie in der vorliegenden Arbeit gezeigt werden soll, können Proxys insbesondere im Rahmen bislang noch weitgehend gewaltloser Cyberkonflikte, die zudem Teil komplexer politischer und wirtschaftlicher Interdependenzen sind, auch demokratischen Staaten durch deren defensive Funktionserfüllung Kosten auf nationaler sowie internationaler Ebene ersparen. Liberal formuliert handelt es sich hierbei um die Manipulation bestehender

4 Diese stärkere Datenorientierung forderten auch Brandon Valeriano und Ryan C. Maness in einem 2018 veröffentlichten Artikel zu den methodischen Herausforderungen der empirischen Cyberkonfliktforschung.

Interdependenzverhältnisse nach innen und außen, die durch den Einsatz von Proxys erreicht werden soll.

Gesellschaftliche Relevanz entfaltet die Arbeit dagegen in folgender Hinsicht (vgl. Gschwend und Schimmelfennig 2007, S. 15): Erstens wird ein zunehmend sekuritisiertes Untersuchungsfeld bearbeitet. Sowohl politische als auch privatwirtschaftliche AkteurInnen zeigen ein stetig steigendes Interesse daran, durch teilweise unverhältnismäßige Formulierungen den Cyberspace als ›Fifth Domain‹ zu kennzeichnen.[5] PolitikerInnen bietet dies die Chance, steigende Sicherheitsbudgets im Cyberspace sowie in Teilen auch kontroverse Eingriffe in die individuelle Privatsphäre eigener und fremder BürgerInnen zu rechtfertigen. Für IT-Unternehmen lohnt es sich, die Anzahl und Schwere stattfindender Cyberangriffe ebenfalls permanent zu betonen, da sie es sind, die mit ihren Produkten Schutz vor den stetig steigenden Gefahren im Cyberspace versprechen. Indem somit eine möglichst breite Datenbasis über (öffentlich bekannte) Cyberoperationen und deren Intensität vorgestellt und analysiert wird, kann die tatsächliche Cyberkonfliktlandschaft besser als auf Grundlage bloßer Einzelfallstudien bewertet werden. Trotz der genannten Sekuritisierung ist unbestritten, dass der potenzielle Angriffsvektor im Cyberspace zunehmend steigt, sei es durch das Internet of Things, die Integration künstlicher Intelligenz in Produkten des privaten sowie öffentlichen Sektors sowie sonstige Digitalisierungsmaßnahmen. Der Cyberspace und dessen Verregelung bzw. der Schutz öffentlicher Systeme, allen voran kritischer Infrastrukturen, stellen somit hohe öffentliche Güter dar, die es vor dieser steigenden Gefahr zu schützen gilt, bei gleichzeitig notwendiger, zielspezifischer Risikoabschätzung. Zweitens kann die vorliegende Arbeit auch das Problemverständnis politischer EntscheidungsträgerInnen im Umgang mit ausländischen HackerInnen stärken. Denn nur, wenn sie ein entsprechendes Verständnis darüber entwickeln, welcher Art die Beziehung zwischen nichtstaatlichen AkteurInnen als Proxys (autokratischer) Staaten sein kann und in den jeweiligen Fällen konkret ist, können auch effektive politische Reaktionsoptionen entwickelt werden. Die Motivlage des Staates sowie des Proxys für die Aufnahme der Beziehung zu kennen, ist hierfür genauso wichtig, wie ein umfassendes Verständnis für die jeweiligen Handlungsrestriktionen dieser AkteurInnen zu entwickeln.

1.2 Bisheriger Forschungsstand zu Proxys im Cyberspace

Damit das avisierte Erklärungsmodell im Kontext bereits existierender Forschungsarbeiten zum Thema der staatlichen (Cyber-)Proxy-Nutzung situiert werden kann (George und Bennett 2005, S. 70), müssen diese zunächst beschrieben werden. Somit können notwendige Modifizierungen etablierter Konzepte begründet werden. Nachfolgend wird zunächst auf die unterschiedlichen Definitionen des Konzepts des Cyberproxys in relevanten Forschungsarbeiten eingegangen. Anschließend wird der Forschungsstand zur Nutzung dieser Cyberproxys in Demokratien und Autokratien näher beleuchtet.

5 Beispiele hierfür sind die Analogien ›Cyber Pearl Harbor‹, ›Cyber-Armageddon‹ oder auch ›World War C‹.

Das Konzept des ›Cyberproxy‹ fungiert generell als Oberkategorie für verschiedene Akteurskategorien. In der Forschungsliteratur wurden bislang hauptsächlich folgende Akteursgruppen als potenzielle TrägerInnen der Proxy-Rolle im Rahmen von Cyberoperationen identifiziert, die entweder durch militärische oder zivilgeheimdienstliche AkteurInnen an den jeweiligen Staat angebunden sein können:

- *Cybermilizen:* Der Term *›Cybermilitia‹* diente bislang als eine Art Sammelbegriff für staatlich gesponserte (Applegate 2011, S. 18), andererseits jedoch auch aus eigenen Stücken agierende, patriotisch gesinnte Zusammenschlüsse organisierter HackerInnen oder auch CybersicherheitsexpertInnen (Dudney 2011), die ad hoc oder permanent geformt werden (Ottis 2010, S. 233). Die jeweiligen Fähigkeiten hängen dabei von den individuellen Kenntnissen und Kapazitäten der Gruppenmitglieder ab (Sigholm 2013, S. 11). Anwendung fand das Konzept bislang vor allem für die Volksrepublik China (Harris 2008; Krekel 2009; Dudney 2011).[6]
- *Patriotische HackerInnen:* Cybermilizen und patriotische HackerInnen unterscheiden sich hauptsächlich in ihrem jeweiligen Organisationsgrad (vgl. Applegate 2011; Dudney 2011). Bei Letzteren besteht keine Hierarchie oder regelmäßige Vernetzung zwischen den einzelnen HackerInnen, gemeinsam haben sie jedoch ihre patriotische Gesinnung, der sie überwiegend mithilfe technisch anspruchsloserer Angriffe wie *Defacement-* und DDoS-Attacken Ausdruck verleihen (Romagna und van den Hout 2017; Whyte 2018).
- In Abgrenzung zum Konzept der HacktivistInnen sticht bei patriotischen HackerInnen deren nationalistische, regierungsaffine Position heraus. Erstere agieren dagegen oftmals in Opposition zum jeweiligen Staat oder verfolgen eine bewusst transnationale, kosmopolitische Agenda (Dahan 2013, S. 53–54).
- *Cyberkriminelle:* Für das Cyberproxykonzept insgesamt gewannen auch Cyberkriminelle und deren Verbindungen zum jeweiligen Heimatstaat in den letzten Jahren zunehmend an Bedeutung. Die schwierige Differenzierung zwischen »*Cyber crime, cyber terrorism and cyber warfare*« (Klimburg 2011, S. 41) rückte dabei besonders in den wissenschaftlichen Fokus. Ähnlich wie bei der Unterscheidung zwischen lose affiliierten patriotischen HackerInnen und organisierten Cybermilizen wurden auch bei Cyberkriminellen verschiedene Organisations- und Hierarchieformen unterschieden und zudem in Bezug zu den oftmals als AuftraggeberInnen fungierenden staatlichen AkteurInnen gesetzt (Broadhurst et al. 2014). Staatlich zumindest geduldete Cyberkriminelle erfahren seit den russischen Ransomware-Operationen gegen US-Infrastrukturen 2021 wieder verstärkt politische Aufmerksamkeit (Wilkie 2021).
- *Private Military Security Contractors (PMSCs):* In der Forschungsliteratur werden zudem PMSCs häufig als stellvertretende Einheiten vor allem demokratischer Staaten behandelt, denen der Einsatz von Gewalt nur zur Verteidigung erlaubt ist und die vor allem logistische Unterstützungsleistungen erfüllen. Deren teilweise unrechtmäßige Gewaltanwendung im Rahmen bewaffneter Konflikte wurde jedoch im Sinne der Schwächung des demokratischen Gewaltmonopols durch Vertragsnehmer wie das US-Unternehmen *Blackwater* zunehmend kritisch diskutiert (Carmola 2010; Nevers

6 Im weiteren Verlauf wird die Volksrepublik China auch als ›VR China‹ oder nur ›China‹ bezeichnet.

2016). Über autokratische PMSCs im Allgemeinen sowie im Rahmen von Cyberkonflikten im Besonderen wurde bislang weitaus weniger publiziert. Russland kann dabei für die Ukraine- und Syrienkriege noch als Ausnahme gelten (u.a. Fainberg 2017; Sukhankin 2018; Marten 2019). Im Fokus der Aufmerksamkeit standen dabei die »*RSB-Group*« (Østensen und Bukkvoll 2018, S. 23) sowie die bekannteste russische PMSC »*Wagner*«. Letztere besitzt laut öffentlichen Berichten eine im Gegensatz zu demokratischen PMSCs größere ideologische Bindung zum russischen Heimatstaat (Bukkvoll und Østensen 2020, S. 2–3). Hinsichtlich einer Cyberproxy-Rollenübernahme könnte diese Regimetypenunterscheidung für den Motivationsfaktor der *Ideologie* somit von zunehmender Bedeutung sein.

Proxys wurden im Cyberspace bislang fast ausschließlich als offensiv agierende, Cyberattacken ausführende AkteurInnen behandelt (Schmitt und Vihul 2014; Maurer 2016; Maurer 2018a; Maurer 2018b; Borghard und Lonergan 2016; Canfil 2016). In seiner Arbeit von 2016 verweist Tim Maurer darauf, dass selbst auf völkerrechtlicher Ebene jedoch noch keine umfassende Definition des Begriffes ›Cyberproxy‹ existiere, auch wenn dieser dort bereits verwendet wurde (in den UNGGE Reports 2013 und 2015). Zudem sei dessen Übersetzung in nicht englischsprachige Kontexte ebenfalls erschwert und nicht weiter spezifiziert (2016, S. 384). In der Folge arbeitete Maurer daher eine Art kleinsten gemeinsamen Nenner bezüglich des Terminus heraus: Damit werde überwiegend auf die Beziehung zwischen einem nichtstaatlichen Akteur (Proxy/Agent) und einem Staat (Prinzipal/Benefactor) angespielt. Diese Akteurskonstellation sei empirisch besonders relevant und somit auch die primär untersuchungswürdige (2016, S. 383). Auch in den Arbeiten von Schmitt und Vihul 2014 sowie Borghard und Lonergan 2016 zur Thematik, die sich ebenfalls an der Principal-Agent-Theorie orientierten, spiegelt sich dieser Konsens wider.

2016 widmete sich Maurer zudem Fragen der rechtlichen Verantwortungszuweisung von Cyberproxy-Aktivitäten: Wann kann ein Staat überhaupt für die Handlungen seines angeblichen Proxys verantwortlich gemacht werden? In diesem Kontext diskutierte er das Konzept der ›Due Diligence‹ (Sorgfaltsverantwortung) und welche Erwartungen an deren Anwendung im Cyberspace realistischerweise geknüpft werden könnten (S. 384).

Im Gegensatz zu diesen primär theoretischen Überlegungen bearbeitete Maurer in seinem Buch »Cyber-Mercenaries« aus 2018 stärker empirische Beispiele offensiver Cyberproxy-Nutzung (2018a, S. 7). Ein Cyberproxy ist nach Maurer ein »*intermediary that conducts or directly contributes to an offensive action that is enabled knowingly, actively or passively, by a beneficiary*« (2018a, S. 31). Dabei bezieht er sich ausschließlich auf AkteurInnen als Proxys, die zu autonomer Entscheidungsfindung befähigt sind, im Gegensatz zu ebenfalls oft als ›Proxys‹ betitelten technischen Hilfsmitteln (2018a, S. 31). Maurer unterscheidet grundlegend drei Formen der Staat-Proxy-Beziehung: ›Delegation‹ beschreibt dabei die engste Anbindung und damit auch das größtmögliche Maß an Kontrolle über einen nichtstaatlichen Akteur im Cyberspace. Als empirisches Fallbeispiel rekurriert der Autor hierbei auf die USA und deren Nutzung von privaten Sicherheitsfirmen zur Planung und Vorbereitung von Cyberangriffen. In der vorliegenden Arbeit wird eine solche Tätigkeit jedoch aus der Cyberproxy-Definition ausgeschlossen, da hierbei der Angriff final immer noch von einer staatlichen Stelle selbst ausgeführt wird und die üblicherweise

angestrebte Plausible Deniability nicht das primäre Ziel der Einbindung dieser privaten AkteurInnen in die sog. »Cyber-Kill-Chain« (Lockheed Martin 2020) sein kann.[7] Dies ist besonders für die Spionage- und Überwachungstätigkeiten der National Security Agency (NSA) der USA von Bedeutung: Die Enthüllungen Edward Snowdens legten offen, welche Rolle private Dienstleister wie Booz Allen Hamilton oder Lockheed Martin bei der Geheimhaltung der Handlungen an sich spielten, indem deren technische Fähigkeiten zur Planung und Vorbereitung seitens der NSA unter einem hohen Maß an »Operational Security« genutzt wurden. Somit stand hier die Verschleierung der eigenen, liberal-demokratischen Prinzipien widersprechenden Praktiken im Vordergrund, gerechtfertigt vor allem durch das in US-Geheimdienstkreisen etablierte Post-9/11-Sekuritisierungsnarrativ NOBUS (»nobody but us«; Perlroth 2021).[8] Dass speziell in demokratischen Staaten die Beauftragung privater Unternehmen in der Regel durch öffentlich sichtbare Verträge formalisiert wird, spricht ebenfalls gegen die Anwendbarkeit des zentralen Proxy-Motivs der plausiblen Bestreitbarkeit.[9] In demokratischen Staaten werden SubunternehmerInnen vor allem zum Zwecke der Geheimhaltung des Angriffes benutzt. Die Geheimhaltung der Beziehung zum Proxy selbst ist dagegen kein zentrales Ziel dieser Interaktion. Durch öffentliche Haushaltsdebatten, Verträge mit den jeweiligen Firmen sowie demokratische Geheimdienstausschüsse erfolgt in diesen Staaten lediglich eine operative, im Cyberraum oftmals notwendige Geheimhaltung der Angriffspläne. Deren Planung und Durchführung werden dabei durch die entsprechend demokratisch legitimierten Institutionen begleitet und auch kontrolliert. Somit soll sichergestellt werden, dass das Gewaltmonopol im Cyberspace immer noch in den Händen des Staates liegt, gleichzeitig jedoch die eigenen Cyberkapazitäten im Rahmen offensiver Operationen trotz demokratischer Beschränkungen und Kontrollinstanzen effektiv arbeiten können. Aus diesem Grunde können beispielsweise die Geheimdienste sowie die mit ihrer Kontrolle betrauten Ausschüsse nie vollständig öffentlich agieren. Dennoch sollen solch institutionelle Checks and Balances die staatliche Hoheit im eigenen Cyberkonfliktaustrag gewährleisten. Für das Beispiel der USA bedeutet dies jedoch, dass die Geheimhaltung der NSA-Überwachung primär nach innen gerichtet war, um eben jene institutionalisierten Kontrollmechanismen umgehen zu können. Hinzu kommt, dass hierdurch ebenso die illegitime Überwachung eigener BürgerInnen geheim gehalten werden sollte. Zwar war diese aus Sicht der US-Regierung zwingend notwendig, um in Folge des 11. Septembers der Infiltration der USA durch potenzielle TerroristInnen entgegen zu wirken. Gleichzeitig

7 Auch aus völkerrechtlicher Sicht werden PMSCs, welche *nicht* in die bewaffneten Streitkräfte durch konfliktive Tätigkeiten integriert sind, als weniger salient bezüglich der Konfliktentwicklung angesehen, da diese wie unbeteiligte ZivilistInnen auch, als NichtkombattantInnen eingestuft werden (Melzer 2008, S. 39). Das Prinzip kann somit auch für das bloße Schreiben eines Malware-Codes, ohne dessen tatsächlicher Ausführung, seitens des privaten Auftragnehmers angewandt werden (Crawford 2013, S. 16).

8 »Nobody but us« sollte aus Sicht der US-Geheimdienste z.B. dazu im Stande und auch legitimiert sein, entdeckte Sicherheitslücken in Netzwerken für Cyberoperationen auszunutzen.

9 So ist beispielsweise für den erwähnten PMC Blackwater bekannt, dass dieser im Zuge seines Einsatzes im Irakkrieg von 2000 bis 2007 öffentliche Aufträge der USA im Wert von mehr als einer Milliarde Dollar erhalten hat (U.S. Government 2007, S. 2).

zeigt die jahrelange Verschleierung dieser Praxis die asymmetrische Verwundbarkeitssituation in der sich Demokratien gegenüber Autokratien und Terrorgruppen befinden. So schützen die eigenen Gesetze nicht nur die eigenen BürgerInnen vor Übergriffen staatlicher Behörden, sondern eben auch ausländische Akteure mit schädigenden Absichten.

Der zweite Beziehungstypus, den Maurer vorschlägt, sieht dagegen eine losere Staat-Proxy-Beziehung vor. Im Rahmen der ›Orchestration‹ wird der Proxy weniger stark durch den ›Beneficiary‹[10] kontrolliert. So kann der Stellvertreter spezifische Zielsysteme und Angriffsmethoden selbst bestimmen. Entscheidend ist jedoch die üblicherweise bestehende ideologische Übereinstimmung zwischen den beiden AkteurInnen (Maurer 2018a, S. 12). Entgegen dem Titel des Buches weicht Maurer hier somit von der rein finanziellen Motivlage der ›Mercenaries‹ (Söldner) ab. Er demonstriert diese Form der Kooperation anhand der Beispiele Iran und Syrien. Letzteres Regime unterstütze die sog. Syrian Electronic Army Berichten zufolge auf ideologischer Ebene, aber anscheinend auch durch die Bereitstellung von Infrastruktur (Al-Rawi und Ahmed K. 2014). Die dritte Beziehungsform des ›Sanctionings‹ bezieht sich auf die passivste Rolle des Prinzipals und sieht diesen lediglich in einer Art ›gewährenden‹ Rolle vor, der ›ein Auge zudrückt‹, wenn der Proxy beispielsweise vom eigenen Staatsterritorium aus eine Cyberattacke auf einen anderen Staat ausübt. Zwar ordnet der Staat diese Attacke nicht an und unterstützt sie auch nicht materiell, er unterbindet sie jedoch auch nicht, wenn sie mit seinen eigenen Interessen übereinstimmt (Maurer 2018a, S. 20). Hierfür wählte Maurer Russland als Fallbeispiel. Ein potenzieller Wandel in der vorherrschenden Staat-Proxy-Beziehung wird darüber hinaus am Beispiel Chinas demonstriert: Laut Maurer verdrängte hier im Laufe der Zeit der Typus der Delegation das zuvor vorherrschende Beziehungsarrangement des Sanctionings.

In ihrer Arbeit aus 2016 verweisen Erica Borghard und Shawn Lonergan ebenfalls auf die Unterscheidung zwischen den Konzepten der ›Mercenaries‹ sowie der ›Proxys‹ und fügen das Konzept der ›Alliances‹ hinzu. Alle drei Konzepte werden zur Beschreibung der Beziehungsform zwischen nichtstaatlichen AkteurInnen und Staaten im Cyberspace herangezogen (Borghard und Lonergan 2016, S. 401–402). Aus Sicht der AutorInnen eignet sich der Terminus des Proxys für eine sinnvolle Beschreibung dieser Beziehung jedoch am besten: ›Allianz‹ sei keine adäquate Wahl, da hiermit meist zwischenstaatliche, durch öffentlich einsehbare Verträge geschlossene Bündnisse beschrieben werden (2016, S. 402). Der Begriff ›Mercenary‹ sei ebenfalls ungeeignet, um das ganze Spektrum an möglichen Beziehungsformen zwischen nichtstaatlichen AkteurInnen und Staaten zu erfassen, da Söldnern seitens der Genfer Konvention (Artikel 47(2)) eine ausschließlich auf finanziellen Gewinn ausgerichtete Motivation zugesprochen wird, sie keine beteiligte Partei des Konfliktes sind, an dem sie teilnehmen, und ebenfalls eine Art öffentliche Beziehungsform darstellen (Borghard und Lonergan 2016, S. 403).

10 Maurer verwendet den Begriff ›beneficiary‹ anstelle von ›principal‹, um aufzuzeigen, dass das Spektrum an möglichen Staat-Proxy-Beziehungen sehr viel weiter gespannt ist, als sie von traditionellen Principal-Agent-Ansätzen dargestellt wird. Somit könne die Bandbreite zwischen ›principal‹ (delegation), ›orchestrator‹ (orchestration) sowie die Rolle des Staates beim ›sanctioning‹ in einem Begriff vereint werden (Maurer 2018a, S. 21).

In der vorliegenden Arbeit wird der Argumentation von Borghard und Lonergan gefolgt, weshalb für eine möglichst tragfähige und inklusive Analyse der möglichen Beziehungsformen zwischen nichtstaatlichen und staatlichen AkteurInnen im Cyberspace das Konzept des Proxys das geeignetste zu sein scheint. Borghard und Lonergan definieren Staat-Proxy-Beziehungen wie folgt: »*A proxy alliance is an agreement between a state and a non-state group that involves the exchange of military resources in furtherance of a political objective*« (2016, S. 404). Somit inkludieren sie die Beziehungsform des Sanctionings aus Maurers Konzept nicht in ihre Analyse, da hierbei kein Transfer materieller bzw. militärischer Ressourcen (auch in Form von Training oder logistischer Unterstützung) vom Staat an den Proxy stattfindet. Ebenso würde die Delegation-Beziehungsform, wie sie Maurer anhand der Kooperation zwischen der US-Regierung und privaten IT-Firmen beschreibt, nicht unter diese Cyberproxy-Definition fallen. Als wichtigsten kleinsten gemeinsamen Nenner stellen Borghard und Lonergan die »*informal, plausibly deniable nature of the relationship*« zwischen Staat und Cyberproxy heraus, die im Falle öffentlich einsehbarer Verträge zwischen IT-Firmen und der US-Regierung nicht gegeben ist (2016, S. 405). In der vorliegenden Arbeit wird die Logik des Sanctionings jedoch im Gegensatz zu den AutorInnen insbesondere in Bezug auf das Attributionsverhalten privater IT-Firmen in Demokratien aufgegriffen. Es wird hierbei von einem indirekteren Delegationsmodus zwischen Staat und Proxy ausgegangen, der ebenfalls lediglich die Tolerierung/passive Ermöglichung der technischen Attributionen bedeuten könnte. Daher wird in der vorliegenden Arbeit die Logik des Sanctionings als potenzielle Staat-Proxy-Beziehungsform inkludiert.

Ferner schließen Borghard und Lonergan Cyberspionage generell aus ihrer Analyse aus, verweisen jedoch selbst auf die Schwierigkeit, isolierte Spionage von Aufklärung zur Vorbereitung einer disruptiveren Cyberattacke aus Sicht des Opfers zu unterscheiden (2016, S. 406). Da Cyberspionage als prävalente Konfliktform im Cyberspace vermutet wird, findet durch deren Inklusion in der vorliegenden Arbeit eine Abgrenzung von den beiden AutorInnen statt.

Als zentrale theoretische Dimensionen verbinden Borghard und Lonergan allianztheoretische Erwägungen mit ihrer Cyberproxy-Definition, indem sie letztere zu internen und externen Sicherheitsdilemmata in Beziehung setzen. Zunächst erstellen sie hierfür eine Proxy-Typologie, worin der Organisationsgrad (individuell/lose vs. organisiert) sowie die jeweilige Motivation (politisch vs. ökonomisch) als zentrale Kategorien verwendet werden (2016, S. 408).[11] Im Rahmen einer zweiten Typologie unterscheiden sie Proxys anhand des jeweiligen Sicherheitsdilemmas, das besonders relevant/präsent ist (extern vs. intern), sowie des jeweils identifizierten, staatlichen Defizits (»Deficit in Capabilities« vs. »Deficit in Willingness«) (Borghard und Lonergan 2016, S. 414). Auf

11 Für den Typ *individuell organisiert* und *ökonomisch motiviert* benennen die AutorInnen jedoch das Beispiel des ILOVEYOU-Wurms aus 2000. Da dem vermeintlichen Täter Onel de Guzman jedoch keine Beziehung/Unterstützung seitens einer Regierung nachgesagt wurde, erfüllt der Fall genau genommen nicht die eigens formulierte Cyberproxy-Definition der AutorInnen.

dieser Grundlage treffen sie sodann Aussagen über die zu erwartenden staatlichen Proxy-Präferenzen.[12]

Neben diesen dominierenden Cyberproxy-Analysen im Sinne offensiv agierender HackerInnengruppierungen untersuchte Florian Egloff in seiner Dissertation zu »Cyber-Privateers & Cyber-Pirates« aus 2018 die Nähe des jeweiligen, nichtstaatlichen Akteurs zum affiliierten Staat.[13] Durch die Verwendung der Seefahrt-Analogie zeigt Egloff auf, in welchen Fällen Staaten versuchen, diese ›*Proximity*‹ in einer gemeinschaftlich genutzten Sphäre zu ihren Gunsten unterschiedlich zu *framen*, wie es auch im transnational funktionierenden Cyberspace der Fall ist (2018, S. 53). Neben den ›Cyber-Privateers‹ und ›Cyber-Pirates‹ untersucht Egloff jedoch auch ›*Mercantile Companies*‹ als nichtstaatliche AkteurInnen mit varianten Beziehungsformen zu staatlichen Stellen. Damit reicht seine Arbeit näher als die meisten anderen im Themenfeld an die in dieser Arbeit konzeptualisierte, primär demokratisch geprägte Proxy-Definition heran. So sieht Egloff in der Zusammenarbeit zwischen US-amerikanischen Technologie-Firmen und der NSA, wie sie 2013 durch Edward Snowden bekannt wurde, ebenfalls eine Form der Kooperation/Interaktion zwischen nichtstaatlichen AkteurInnen und Staaten im Cyberspace.

Da in der Forschung die Beziehung zwischen Staat und Proxy zumeist einseitig konzeptualisiert werde, stelle das Cyberproxy-Konzept für seine eigene Arbeit nur einen unzureichenden Analyserahmen dar, so Egloff (2018, S. 20). Dagegen betonten andere BeobachterInnen im Kontext, dass der Kern einer Staat-Proxy-Beziehung analog zur Principal-Agent-Theorie auch im Cyberspace auf *gegenseitigem* Nutzen beruhe und somit sehr wohl auch in der Lage sei, die unterschiedlichen Motivlagen des nichtstaatlichen Akteurs zu erfassen (z.B. Borghard und Lonergan 2016, S. 405–406). Die in dieser Arbeit vertretene Perspektive stimmt mit dieser zuletzt beschriebenen Ansicht überein.

Weitere Arbeiten, in denen defensivere Funktionen nichtstaatlicher AkteurInnen im Cyberspace unter staatlicher Duldung oder Anleitung thematisiert wurden, sind die Beiträge von Kristen Eichensehr aus den Jahren 2017, 2019 und 2020 sowie die Arbeiten von Romanosky 2017 sowie Romanosky und Boudreaux 2021. Diese deuteten erstmals auf den Mehrwert, aber auch die potenziellen Risiken der von IT-Firmen getätigten Attributionen für demokratische Regierungen hin, auch wenn erstere dabei nicht als Proxys benannt wurden.[14]

---

12 Dabei werden zwei unterschiedliche Staat-Proxy-Beziehungsformen Russlands (einerseits zum Russian Business Network und andererseits zu patriotischen HackerInnen) als Beispiele für sowohl das Wirken des externen, als auch des internen Sicherheitsdilemmas herangezogen. Dies lässt die Frage offen, wann welchem von beiden die größere Wirkmacht seitens des Staates zugesprochen wird und es somit zu unterschiedlichen Proxy-Nutzungsstrategien kommt.

13 Auch Egloff spricht (wie Maurer) nicht ausschließlich von Cyberproxies. Aufgrund der vorgestellten theoretischen Überlegungen lässt sich seine Arbeit zu nichtstaatlichen AkteurInnen im Cyberspace dennoch in den dazugehörigen Forschungsstrang einordnen.

14 Auf besagte Arbeiten wird im Zuge der Entwicklung des demokratischen Cyberproxy-Ansatzes im weiteren Verlauf noch genauer eingegangen.

1.3 Vergleich konventioneller und Cyberproxy-Funktionslogiken

Beim Vergleich von traditioneller Forschung mit der Cyberproxy-Forschung lassen sich folgende Unterschiede feststellen:

Die Überbrückung geografischer Distanzen ›at light speed‹
Für Proxy-Aktionen im Cyberraum ist es nicht notwendig, einen (offensiven) Proxy zu verwenden, der im Gebiet des Ziellandes stationiert ist.[15] Im Gegenteil: Immer mehr empirische Arbeiten zeigen, dass (hauptsächlich) autokratische Staaten nationale HackerInnen anheuern, anstatt die Mission an ausländische AkteurInnen auszulagern, über die sie keinerlei Kontrolle haben (für Iran: Anderson und Sadjadpour 2018; Russland: Carr 2011; Connell und Vogler 2017; China: Raud 2015).[16] Zudem kann die Versorgung der Proxy-AkteurInnen mit technischer Unterstützung erfordern, dass sie sich auf dem Territorium des Auftraggebers befinden, da nur hier die volle Kontrolle über die IT-Infrastruktur gegeben ist (Borghard und Lonergan 2016, S. 407). Außerdem ist es aus operativer Sicht für die Durchführung der meisten Cyberangriffe schlicht nicht notwendig, dass sich ein Proxy-Akteur im Land des anvisierten Ziels befindet (Brenner 2007).

Bezüglich des Spektrums staatlicher Verantwortlichkeit stellt die bloße Duldung der Tätigkeit von Proxys vom eigenen Staatsterritorium aus somit die niedrigschwelligste Staat-Proxy-Beziehung im Cyberspace dar, wie es vor allem im Hinblick auf Ransomware-Operationen russischer Cyberkrimineller seit 2021 verstärkt diskutiert wird (vgl. Hunnicutt 2021). Die im Falle traditioneller Proxys aktivere Unterstützung seitens des staatlichen Auftraggebers stellt somit einen weiteren Unterschied zur wissenschaftlichen Betrachtung von Cyberproxys dar, die von ihrem Staat auch lediglich geduldet werden können.

Aus dieser umgekehrten Stationierungslogik ergibt sich zudem, dass Cyberproxys im Gegensatz zu analogen Proxys zumeist in keinem Konflikt mit dem anvisierten Akteur stehen, also erst durch die Beauftragung des Staates zu einer Konfliktpartei werden. Eine Ausnahme hiervon sind vor allem patriotische HackerInnen und Cybermilizen.

AkteurInnen mit breitem Motivationsspektrum
Im Gegensatz zu ihren analogen Pendants weisen Cyberproxys ein noch vielfältigeres Spektrum an potenziellen Motiven für die eigene Rollenübernahme auf: Das ›MICE‹-Akronym (Money, Ideology, Coercion, Ego; Eoyang 1994), das zur Beschreibung der Motivationen konventioneller Spione verwendet wird, kann auch bei ihnen Anwendung finden. In der Literatur wird besonders von einigen ›Hired-Gun‹-Gruppierungen ausgegangen, etwa dem Russian Business Network (RBN), die bei entsprechender Bezahlung für nahezu jeden Auftraggeber arbeiten (Money) (vgl. Klimburg 2011, S. 49–50). Daneben existiert jedoch auch eine große Bandbreite an staatlich geförderten HackerInnen, die aus ideologischer Überzeugung oder Interessenskompatibilität an ihre Mission glauben (Ideology) (vgl. Staniland 2015).

15 »*Electrons are cheaper, faster, safer, and more easily deniable than human spies*« (Nye 2018).

16 Die bekannteste Ausnahme von dieser Praxis ist Nordkorea, welches vor allem in China, Indien aber auch Russland stationierte Proxys für Cyberattacken nutzt (Insikt Group 2017a).

Neben auf Freiwilligkeit basierenden Motiven nichtstaatlicher AkteurInnen können jedoch auch staatliche Zwangsmaßnahmen diese zur Proxy-Rollenübernahme bewegen. Bei einem kriminellen Aktivitätsprofil des Proxys kann diesem Strafe angedroht werden, falls er nicht auch Aufträge der jeweiligen Regierung übernimmt (Coercion). Schließlich kann das Ego der StellvertreterInnen ihr Engagement erklären: Für technisch ambitionierte HackerInnen offeriert die finanzielle und technische Unterstützung eines Staates ungeahnte Möglichkeiten bei der Durchführung von Cyberoperationen. Ein Handeln im Rahmen einer geheimen Staatsoperation kann zudem das Geltungsbedürfnis solcher AkteurInnen in besonderem Maße stärken. Dasselbe gilt auch für IT-Firmen, die in demokratischen Staaten durch zunehmend sophistizierte Attributionsberichte nicht nur ihre Gewinnmarge, sondern auch ihre Reputation im Allgemeinen stärken können. Zudem dürfte entsprechend des eigenen Selbstverständnisses als liberal-demokratisches Unternehmen auch eher solchen Regierungen durch die eigenen Aktivitäten gedient werden wollen.[17]

Verschleierung durch ›Plausible Deniability‹ (›plausible Abstreitbarkeit‹)

Der wichtigste (aber nicht ausschließliche) Vorteil, den ein Cyberproxy einem Staat bieten kann, ist die Schaffung der bereits erwähnten ›Plausible Deniability‹, wodurch letztlich die eigene Verantwortlichkeit verschleiert werden soll.[18] Dies gilt insbesondere für autokratische Staaten, die versuchen, ihre schadhaften Cyberaktivitäten durch die Anweisung und/oder Unterstützung eines dritten Akteurs zu verdecken. Im Gegensatz zu demokratischen Staaten haben Autokratien aufgrund ihrer illegitimen Cyberoperationen sowie der strukturellen Dominanz demokratischer Wert- und Normvorstellungen auf der Ebene der internationalen Beziehungen mehr Angst vor internationalen Rückschlägen als vor ihrer heimischen Bevölkerung.[19] Die Aufgabe des

17 Gestützt werden diese Annahmen auch durch den Artikel von Romanosky und Boudreaux aus 2021: Darin führten diese ExpertInneninterviews durch, um die unterschiedlichen Motivlagen privater und staatlicher AkteurInnen für öffentliche Cyberattributionen zu beleuchten. Die Befragten verwiesen für IT-Firmen vor allem auf deren Reputationsgewinne, aber auch deren Ansinnen, die breite Öffentlichkeit für Bedrohungen im Cyberspace zu sensibilisieren und somit die Debatte informierter zu gestalten.

18 Diese wird jedoch seitens Andrew Mumford auch für den Einsatz analoger Proxies als *ein* zentrales Motiv staatlicher Prinzipale in seinem Buch aus 2013 herausgestellt. Unter ›Verschleierung‹ wird im Rahmen der Arbeit eine gezielte Herstellung oder Manipulation bestehender Informations(a)symmetrien verstanden. Damit müssen nicht notwendigerweise eine völlige Geheimhaltung der eigenen Handlung bzw. Verantwortlichkeit hierfür einhergehen.

19 So zeigt das Beispiel Stuxnet, dass demokratische Staaten wie die USA und Israel aufgrund ihres schadhaften Cyberengagements gegen ›Schurkenstaaten‹ wie den Iran bislang keine internationalen Sanktionen oder Konsequenzen fürchten mussten. Auch wenn unilateral nahezu sämtliche demokratische StaatsführerInnen derlei Angriffe auf die kritische Infrastruktur eines anderen Landes generell verurteilt haben, so hat die demokratische Allianzkonstellation eine öffentliche Verurteilung der Cyberaktionen des Verbündeten (der zudem auf allen Ebenen überlegen/asymmetrisch mit Machtressourcen ausgestattet ist) bislang verhindert. Hinzu kommt, dass es neben den unilateralen Verurteilungen bislang noch zu keiner multilateralen, verbindlichen Erklärung über das Verbot von Cyberangriffen auf kritische Infrastrukturen gekommen ist, die über die UNGGE Berichte 2013/2015 hinaus geht.

legitimen Gewaltmonopols nach Max Weber ist, wie Maurer 2018a betont, für demokratische Regierungen weitaus kritischer als für ihre autokratischen Pendants, wenn auch ›nur‹ im Cyberspace.[20] Einen offensiven Cyberproxy zu verwenden, kann Autokratien somit vor bi- oder multilateralen Sanktionen schützen. Die selektive Strafverfolgung staatlicher HackerInnen wird dabei oftmals in Kauf genommen.

1.4 Staatliche Cyberproxy-Nutzung als rein offensives Metier?

Der Literaturüberblick und der Vergleich zeigen, dass sich die Proxy-Forschung bislang überwiegend auf die offensive Rolle nichtstaatlicher AkteurInnen fokussierte. Während in konventionellen Konflikten in erster Linie lokale Proxys unterstützt wurden und der staatliche Sponsor in den meisten Fällen eigentlich keine direkte Konfliktpartei ist, werden Proxys im Cyberspace vor allem genutzt, um andere Staaten mit oder ohne darunter liegendem konventionellen Konflikt zu schwächen oder zielunspezifische Vorteile durch den Angriff zu generieren (Cyberspionage). Das Motiv der Plausible Deniability scheint dabei für den Cyberspace eine noch größere Relevanz zu entfalten, begünstigt hier vor allem durch das noch zu behandelnde Attributionsproblem.

Der grundlegenden Proxy-Logik, im Sinne einer angestrebten Kostenvermeidung durch einen zwischengeschalteten Stellvertreter, folgen der Argumentation der Arbeit nach jedoch nicht nur autokratische Staaten. So haben Demokratien gerade aufgrund ihres Status als prominente Ziele autokratischer Cyberangriffe ein Interesse daran, die mit der Beantwortung dieser Vorfälle verbundenen Kosten durch den Einsatz defensiver Proxys regelmäßig zu vermeiden. Beide Cyberproxynutzungen interagieren somit und treffen als regimetypenspezifische Außenpolitiken auf außenpolitischer Ebene aufeinander. Im weiteren Verlauf der Arbeit wird auf demokratischer Seite insbesondere das Delegieren oder Anstoßen privat geführter Attributionsbemühungen seitens IT-Firmen als eine solch defensive Proxytätigkeit betrachtet. Hierfür wird auch geklärt werden, warum gerade dieser Aktivität besondere politische Bedeutung im Hinblick auf Kostenvermeidung demokratischer Regierungen zugesprochen wird. Im Sinne des liberalen Erklärungsansatzes wird somit aufgezeigt, welchen Nutzen diese defensiven Cyberproxys

20 Die nationalen und internationalen Gesetze der meisten demokratischen Staaten verbieten den Einsatz nichtstaatlicher Akteure in der Endphase der Verwaltung offensiver Cyberoperationen. Beispiele hierfür sind das US-Computerbetrugs- und Missbrauchsgesetz oder in Deutschland der sog. Hackerparagraph aus dem Jahr 2007 (§202 c, Strafgesetzbuch der Bundesrepublik Deutschland). Dagegen sind die meisten autokratischen Staaten wie Russland oder China früheren multilateralen Abkommen zur Regulierung von Cyberhacking-Bemühungen vom eigenen Territorium aus nicht beigetreten, wie der Budapester Cybercrime-Konvention aus 2001, einer Initiative des Europarates Grant 2012, S. 16.
Robert Gorwa und Max Smeets stellten folgende These auf: »*Based on the Plausible Deniability argument, we should expect democracies, as states with high levels of public accountability and greater attentiveness to reputational costs than authoritarian regimes, to primarily rely on these types of actors* [cyberproxies; Anm. d. Autorin]« 2019, S. 19. Somit handelt es sich hier um ein republikanisches Gegenargument zur These der beiden Autoren.

demokratischen Regierungen im zunehmend asymmetrisch geführten (Cyber-)konfliktaustrag gegenüber Autokratien bieten. Zudem wird begründet, warum der Begriff ›Proxy‹ im Attributionskontext gerechtfertigt erscheint und warum diese Art von StellvertreterInnen als kritischer und somit untersuchungswürdiger als demokratische Software-Unternehmen bewertet wird, die ihre Technologie nicht nur an autokratische Regierungen verkaufen.[21] Hierfür gilt es jedoch, zunächst das Attributionsproblem als technischen und politischen Untersuchungsgegenstand zu thematisieren.

1.5 Bisheriger Forschungsstand zum Attributionsproblem im Cyberspace

Cyberoperationen verdeutlichen die Besonderheit der einzigen von Menschen selbst erschaffenen »Fifth Domain« (Healey und Wilson 2012, S. 59). Die Grundkonzeption des Cyberspace, jedoch auch der fortschreitende technologische Fortschritt, erweitern das Angriffsspektrum potenzieller Cyberangreifer stetig und erlauben es ihnen, Angriffe weitgehend unerkannt und oftmals auch unentdeckt durchführen zu können. Wichtig ist, dass Attribution ›Detection‹ voraussetzt: Wenn der Angriff gar nicht erst entdeckt wird, weil die AngreiferInnen so subtil und technisch ausgefeilt agierten, kommt das sog. Attributionsproblem nicht zum Tragen, da die Frage nach dem Täter ohne erkennbare Tat gar nicht erst gestellt wird (Baram und Sommer 2019). Somit repräsentieren technische Methoden des Unerkanntbleibens die erste Hürde eines möglichen Attributionsprozesses. Prinzipiell können Methoden der ›*Internal Detection*‹ hierbei Abhilfe schaffen. Dabei handelt es sich etwa um ›Pattern-Matching‹ oder ›Signature-based Detection‹, wodurch als schadhaft einzustufende Netzwerkaktivitäten früher und besser erkannt werden können (Buchanan 2017, S. 56).

Sogenannte ›False-Flag‹-Attacken werden gemeinhin als eine der hauptsächlichen Herausforderungen der Attribution auf technischer, nachgelagert jedoch auch politischer Ebene angeführt. Hierbei verwenden AngreiferInnen technische Tools, die üblicherweise anderen AkteurInnen zugesprochen werden, um so eine falsche Fährte zu legen (Bartholomew und Guerrero-Saade 2016). Technische Methoden wie die Verwendung von Proxy-Servern zum Umleiten des mit dem Angriff verbundenen Datentransfers über Transitländer (Green 2016, S. 114–115) sowie die Instrumentalisierung fremder

21 Ein Unterschied existiert dennoch auch hier zwischen Demokratien und Autokratien: Während der Erwerb und die Nutzung kommerzieller Spionagesoftware von Firmen wie Gamma International oder der NSO-Group seitens demokratischer Staaten lange Zeit weniger kritisch diskutiert wurden, widmet sich etwa das Citizen Lab aus Toronto explizit in seinen Analysen autokratischer Spionagetätigkeit mithilfe solcher Software, da sich diese häufig gegen Dissidenten im In- und Ausland richten. Eine solche Nutzung ihrer Produkte schließen die internen Richtlinien besagter Firmen eigentlich aus und weisen jedwede Verantwortung für potenziellen Missbrauch von sich (Muth 2019). Die angebliche Nutzung der Pegasus-Spyware der NSO-Group seitens der spanischen Regierung gegen einen katalanischen Oppositionellen, aufgedeckt im Juli 2020, war jedoch ein erstes Indiz für das Aufbrechen dieser Regimetypenunterscheidung, welche durch die weiteren Enthüllungen im Sommer 2021 zur Pegasus-Nutzung demokratischer Akteure, darunter auch das deutsche BKA, weitere Nahrung erhielt (Flade und Mascolo 2021).

Computer zum Aufbau eines Botnetzes sind nur zwei weitere Beispiele potenzieller Verschleierungstaktiken (Knake 2010, S. 10).

Trotz aller existierender Vorteile für AngreiferInnen gibt es jedoch auch Grund zur Hoffnung aufseiten der IT-AnalystInnen: Die technischen Möglichkeiten zur Attribution wurden in den vergangenen Jahren erweitert, was nicht zuletzt auch der teilweise stattfindenden Kooperation verschiedener IT-Firmen zu verdanken ist.[22] Technische Indikatoren müssen jedoch zumeist mit geheimdienstlichen oder allgemeinen, politischen Argumenten und Evidenzen verknüpft werden, um Aussagen über die akteursbezogene Identität der AngreiferInnen tätigen zu können. Gerade das Ausmaß technischer Sophistiziertheit in Verbindung mit der funktionalen Ausrichtung der Attacke kann erste Erkenntnisse über den Angreifertyp liefern. Somit können oftmals weniger anspruchsvolle, weil opportunistischer agierende AkteurInnen, etwa Cyberkriminelle, aus dem Kreis der Verdächtigen ausgeschlossen werden. Ist für einen Angriff eine rein finanzielle Motivation auszuschließen, weist der Vorfall jedoch ein hohes Maß an technischer Komplexität auf,[23] wird meist eine staatliche Beteiligung unterstellt, insbesondere seit dem Bekanntwerden von Stuxnet (Guitton und Korzak 2013). Somit wurden rein technische Indikatoren in den politischen Gesamtkontext gestellt bzw. Erkenntnisse über Täter-Mittel-Zusammenhänge auf diesen übertragen und miteinander verknüpft. Weitere Indikatoren, die auf technischer Ebene oftmals mit generellen Evidenzen über die vermuteten TäterInnen verbunden werden, sind »*specific email addresses, certain patterns, specific name files, MD5 hashes, time stamps, custom functions and encryption algorithms*« (FireEye 2014, S. 29) sowie »*timestamps*«, »*strings*«, »*debug paths*«, »*metadata*« oder auch »*passwords*« (Bartholomew und Guerrero-Saade 2016, S. 1–2). Der Mehrwert dieser kontextbasierten Methode wird seitens Forschung (Rid und Buchanan 2015) und Politik (ODNI 2018) propagiert, um einen Ausweg aus der vermeintlich unüberwindbaren Hürde der »*True Attribution*«, also der konkreten Benennung von Akteurstypus und Herkunftsland, zu liefern (Lee 2016).

Darüber hinaus werden jedoch zunehmend die politischen Unwägbarkeiten von Attribution und deren öffentlicher Vermittlung seitens staatlicher, aber auch privater AkteurInnen in den Mittelpunkt öffentlicher Debatten gerückt (Lindsay 2015; Lohmann 2018; Poznansky und Perkoski 2018; Schulzke 2018; Romanosky und Boudreaux 2021). Die bereits beschriebenen technischen, damit verbunden jedoch auch strategischen Unterschiede verschiedener Attributionsarten standen dabei genauso im Mittelpunkt wie die unterschiedlichen Attributionslogiken vor, während und nach einer Attacke (Clark und Landau 2010). Andere BeobachterInnen stellten zunehmend auch die (geo-)politischen Abwägungen während dieser verschiedenen Attributionsstufen in den Mittelpunkt der Debatte, verbunden mit der Frage nach den Interessenlagen der jeweiligen Regierungen (Lin 2016). Aus sozialkonstruktivistischer Sicht wurde dagegen bereits die

22 Ein Beispiel hierfür ist der gemeinsame Bericht verschiedener IT-Firmen mit dem Titel »*Operation Blockbuster*« aus 2016, welcher sich im Zuge des Sony-Hacks mit der nordkoreanischen APT Lazarus beschäftigte (Novetta 2016).

23 Technische Indikatoren hierfür wären etwa die Verwendung von Zero-Day-Exploits oder gestohlener Software-Zertifikate (Saalbach 2019, S. 288).

soziale Konstruktion vermittelter Zusammenhänge zwischen dem Attributionsproblem und staatlichen Deterrence-Strategien thematisiert (Lupovici 2016).[24]

In der Forschung wurde in den letzten Jahren verstärkt die Frage thematisiert, welche Faktoren die jeweiligen Regierungen im Falle einer Cyberoperation auf nationale Zielsysteme zu einer *bewussten* Offenlegung und darüber hinaus zu einer Attribution bewegen können (Poznansky und Perkoski 2018; Baram und Sommer 2019; Canfil 2020). Den bislang umfassendsten Versuch einer Konzeptualisierung staatlicher Attributionsstrategien unternahmen Florian Egloff und Max Smeets 2021: In ihrem Artikel entwickelten sie ein ›Framework‹ für öffentliche Attributionsprozesse, das den Entscheidungsprozess politischer EntscheidungsträgerInnen anhand unterschiedlicher Kategorien abbilden soll (»*Geopolitics*«, »*Intelligence*«, »*Incident Severity*«, »*Handling und Follow-on-Actions*«). Die hierbei erfassten operationsspezifischen, opfer- und angreiferspezifischen sowie kontextspezifischen (Timing und Beziehung zum attribuierten Akteur) Kriterien verdeutlichen die auch im Rahmen dieser Arbeit betonte Multidimensionalität öffentlicher Attributionsprozesse. Diese lassen sich eben nicht nur auf technische Indikatoren und Beweisführungen reduzieren, sondern werden immer stärker zum Gegenstand politischer Abwägungsentscheidungen auf nationaler und internationaler Ebene.

Für weitere Arbeiten spielten zudem demokratietheoretische Implikationen der Cyberattribution bereits eine Rolle. Dabei wurden speziell unzureichende Transparenzstandards der Regierungen im jeweiligen Prozess sowie deren Einfluss auf die Bedrohungsperzeptionen der Bevölkerungen problematisiert (Schulzke 2018). Aber auch die Rolle der Wissenschaft für einen wirksameren, öffentlichen Attributionsprozess wurde in den Mittelpunkt der Debatte gerückt, besonders im Hinblick auf angezweifelte Verantwortungszuweisungen (Egloff 2020a). Bis auf die beiden letztgenannten Quellen konzentrierten sich die bisherigen Arbeiten somit mehrheitlich auf die Rolle politischer Eliten im Rahmen von Cyberattributionsprozessen. Die potenziell steigende Bedeutung privatwirtschaftlicher AkteurInnen zur Kommunikation von Verantwortungszuweisungen auch gegenüber fremden Staaten wurde insbesondere durch die Arbeiten von Kristen Eichensehr aus den Jahren 2017, 2019 und 2020 stärker präsent. Daran anknüpfend untersuchten Sasha Romanosky und Benjamin Boudreaux 2019 die zunehmende Verflechtung zwischen politischen und privaten AkteurInnen bei der öffentlichen Aufarbeitung von Cyberoperationen, gestützt durch ExpertInnen-Interviews mit beiden Stakeholdergruppen.

1.6 Forschungsdesign

Im Rahmen eines regimetypenbasierten Erklärungsmodells wird in der Arbeit untersucht, welche Rolle und Funktionen nichtstaatliche AkteurInnen in den Cyberstrategien nationaler Staaten übernehmen können. Hierfür wird ein liberaler Erklärungsansatz

24 Dabei ging es konkret um die soziale Vermittlung von Bedeutungszusammenhängen der Konzepte ›Gewalt‹ und ›Anonymität‹ und welchen Einfluss diese sozialen Konstruktionen auf den Erfolg oder das Scheitern von ›cyber-deterrence‹ nehmen.

angeboten. Für Autokratien bedeutet dies die Proxy-Funktion offensiver Cyberoperationen, für Demokratien die Proxy-Funktion defensiver Attributionsbemühungen. Entsprechend der jeweils unterschiedlichen Regime-Logiken autokratischer und demokratischer Staaten beim Einsatz von Cyberproxys werden die Kosten, die von den als Cyberproxys auftretenden AkteurInnen anstelle des Staates getragen werden, unterschiedlich konzeptualisiert. Dies hat wiederum Einfluss auf die Frage, wer jeweils als staatlicher Proxy im Cyberspace zu gelten hat und wer nicht. ›Cyberproxys‹ werden definiert als *offiziell nichtstaatliche AkteurInnen, die für eine (oder mehrere) Regierung(en) eine Handlung im oder den Cyberspace betreffend ausführen, die ansonsten die Regierung selbst hätte tätigen müssen, was für Letztere mit hohen, regimetpyenabhängigen Kosten verbunden sein kann.* Anlehnend an Borghard und Lonergan (2016) und in Kontrast zu Maurers Definition werden somit auf autokratischer Seite lediglich vorbereitende Dienstleistungen im Hinblick auf eine solche Handlung *nicht* erfasst, weil hierbei letztlich die jeweilige Regierung final operativ tätig wäre. Ein Beispiel hierfür wären Software-Firmen, die Regierungen Spionagesoftware liefern, diesen jedoch keine Plausible Deniability bieten können, da die Ausführung der Cyberoperation letztendlich bei den staatlichen Einheiten verbleibt. Zudem verkaufen die erwähnten IT-Firmen öffentlichen Erkenntnissen nach ihre Produkte sowohl an Demokratien als auch an Autokratien. Regimetypenabhängige Faktoren scheinen hier somit weniger relevant zu sein.

Ähnlich wie bei Borghard und Lonergan wird in vorliegender Konzeptualisierung die unterschiedliche Motivlage nichtstaatlicher AkteurInnen betont, sich in die Rolle eines autokratischen Proxys zu begeben. Im Gegensatz dazu steht die einseitigere Konzeptualisierung der nach finanziellem Profit strebenden ›Cyber-Mercenaries‹.

Im Anschluss an das erste Kapitel wird der ›neue Liberalismus‹ nach Andrew Moravcsik als gewählter Theorierahmen diskutiert. Besonderer Fokus liegt dabei auf den gesellschaftlichen Interessen im Sinne der dreigliedrigen Ausdifferenzierung sowie den Interdependenzen als der von Moravcsik als zentral erachteten Präferenzkonstellation auf internationaler Ebene. Es sollen die Fragen beantwortet werden, inwiefern liberale Erklärungsansätze bisher in der Lage waren, konfliktive vs. kooperative Außenpolitiken demokratischer und autokratischer Staaten auf Grundlage welcher Prämissen zu erklären, wie sich der Ansatz des ›neuen Liberalismus‹ von den beiden Theoriesträngen des Institutionalismus und Realismus abgrenzt und warum er für das Erkenntnisinteresse der Arbeit als am sinnvollsten erachtet wird. Nachfolgend wird aufgezeigt, inwiefern die vorliegende Arbeit das Eigeninteresse politischer Führer noch stärker in den Mittelpunkt der Analyse stellt als Moravcsik und inwiefern hierdurch eine Manipulation von asymmetrischen Interdependenzverhältnissen nach innen und außen möglich wird. Dabei sollen folgende Fragen adressiert werden: Welche liberalen Hypothesen erscheinen auch für politische Handlungen im Cyberspace plausibel? Welche notwendigen Anpassungen müssen auf theoretischer Ebene vorgenommen werden, um dem Cyberspace als Konfliktaustragungsraum gerecht zu werden und außenpolitisches Verhalten hierin aus liberaler Perspektive heraus plausibilisieren zu können?

Nachfolgend werden die unterschiedlichen Chancen zur Durchsetzung eigener Interessen bzw. die strategischen Handlungsspielräume autokratischer und demokratischer Regierungen im bzw. mithilfe des Cyberspace gegenüber ihrer domestischen und internationalen Umwelt behandelt. Auf Grundlage dieser theoretischen Vorar-

beiten wird im dritten Kapitel das liberale, regimetypenabhängige Erklärungsmodell staatlicher Cyberproxynutzungsmuster konzeptualisiert. Dabei wird erläutert, welche Rolle unterschiedliche Cyberproxys bei der Manipulation antizipierter oder bereits bestehender asymmetrischer Interdependenzverhältnisse aus autokratischer und demokratischer Perspektive spielen können. Die zentrale unabhängige Variable des Erklärungsmodells stellen die jeweiligen domestischen Präferenzkonstellationen im Sinne Moravcsiks dar, da diese Ausdruck der Interessensdurchsetzungschancen verschiedener AkteurInnen auf republikanischer Ebene sind und aufzeigen, welche ideellen und wirtschaftlichen Präferenzen des Staates dies auf außenpolitischer Ebene zur Folge hat. Es wird zudem begründet, warum die jeweilige Umwelt des im Cyberspace agierenden Staates als konditionierende Variable sowie das allgemeine Konfliktniveau von Cyberkonflikten als intervenierende Variable bedeutsam sind. Die abhängige Variable der staatlichen Cyberproxy-Strategie wird nochmals unterteilt in Funktion und Art der Proxys, d.h., welche inhaltlichen Aufgaben sie für den staatlichen Auftraggeber übernommen haben und durch welche Akteurscharakteristika sie sich beschreiben lassen. Letztlich werden über das Wirken dieser einzelnen Bestandteile Hypothesen formuliert, die es im Rahmen der empirischen Analyse zu überprüfen gilt.

Als Hauptinstrumentarium hierfür wird ein Mixed-Methods-Ansatz verwendet: Auf Grundlage eines umfassenden Cyberkonfliktdatensatzes (HD-CY.CON) werden zunächst die übergeordneten Trends getestet: Nutzen tatsächlich in erster Linie autokratische Staaten offensive Cyberproxys gegen demokratische Staaten und sind es primär demokratische Länder, in denen IT-Firmen den Attributionsprozess übernehmen? Zudem soll geprüft werden, ob sich die bislang etablierte Vorstellung von staatlicher Zurückhaltung im Cyberspace auch auf Grundlage des HD-CY.CON bekräftigen lässt. Diese wurde bislang über rationale Kosten-Nutzen-Erwägungen der AkteurInnen erklärt, wobei die Effektivität von Cyberoperationen im Vergleich zu traditionellen Konfliktaustragungsmitteln angezweifelt wurde (Gartzke 2013; Valeriano et al. 2018; Borghard und Lonergan 2019). Eine zweite, sozialkonstruktivistisch geprägte Perspektive würde dagegen stärker die einhegende Wirkung bereits etablierter oder emergierender Normen im Cyberraum als Wirkfaktor herausstellen, gerade im Hinblick auf das bisherige Ausbleiben von Cyberangriffen mit letalen Folgen (Finnemore und Hollis 2016). Ein dritter Erklärungsansatz macht dagegen die Furcht vor ungewollten, analogen Eskalationsdynamiken primär für die bisherige Zurückhaltung von Staaten im Cyberspace verantwortlich (Valeriano und Maness 2014; Valeriano und Jensen 2019). Zuletzt wertet die neorealistische Perspektive die staatliche Zurückhaltung im Cyberspace als bloßes Nebenprodukt der globalen Machtverteilung nach dem Ende des Kalten Krieges (Healey und Jervis 2020). In vorliegender Arbeit wird stattdessen argumentiert, dass eine bislang dominante Zurückhaltung autokratischer sowie demokratischer Staaten im Cyberspace in erster Linie als interdependentes Produkt der jeweiligen Proxy-Strategien angesehen werden kann, deren Analyse das hauptsächliche Erkenntnisinteresse der Arbeit darstellt.

Wurde die Fallauswahl getroffen, erfolgt die empirische Analyse im Rahmen eines strukturiert-fokussierten Vergleiches nach George und Bennett (2005). Die hierfür abgeleiteten Vergleichsfragen dienen dabei in allen Fällen als implizit strukturierende Elemente der späteren Analyse. Unterstützt werden sollen die vier Fallstudien (auf auto-

kratischer Seite: Russland und China; auf demokratischer Seite: USA und Israel) für den Zeitraum von 2000–2019 durch einzelne, halbstrukturierte ExpertInneninterviews, deren Erkenntnisse neben Informationen aus Primär- und Sekundärliteratur aus Wissenschaft, Politik und IT-Sektor in die empirische Analyse einfließen.