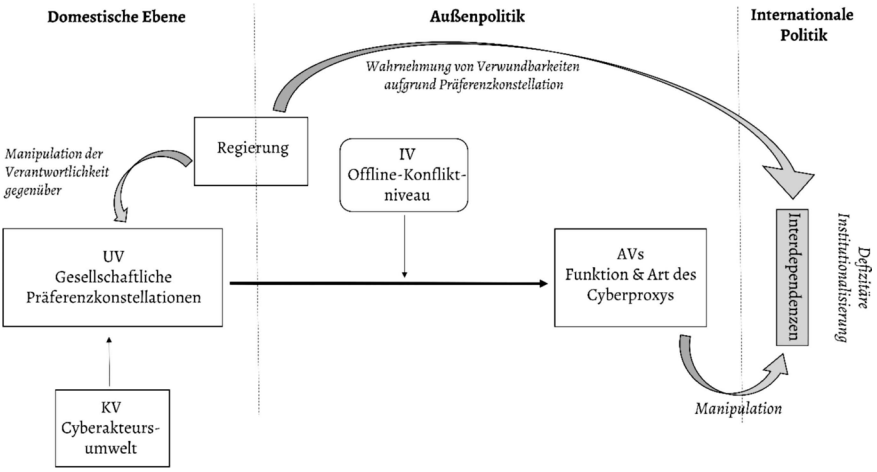
3. Ein liberales Erklärungsmodell staatlicher Cyberproxy-Strategien

Demokratische und autokratische Regierungen sehen sich – wie aufgezeigt – unterschiedlichen Herausforderungen im außenpolitischen Bereich sowie zunehmender Digitalisierung gegenüber. Der immer grenzüberschreitendere Charakter sozialer, politischer, militärischer sowie wirtschaftlicher Maßnahmen führte dabei zwar zu einer prinzipiellen Kriegsaversion, jedoch gleichzeitig zur immer stärkeren Umkämpftheit aller genannter Domänen, um im globalen Geflecht aus wechselseitigen Abhängigkeiten nicht regelmäßig ins Hintertreffen zu geraten (vgl. Wright 2017). Im Umgang mit diesen asymmetrischen Interdependenzen bedingen – neben der bislang defizitären Institutionalisierung im Cyberbereich – variante Wirkfaktoren auf domestischer Ebene im Sinne ideeller, wirtschaftlicher sowie republikanischer Merkmale regelmäßig unterschiedliche Außenpolitiken. Welche Rolle speziell Cyberproxys für beide Regimearten sowie deren Subtypen im Umgang mit den wahrgenommenen Vulnerabilitätsasymmetrien in interdependenten Präferenzkonstellationen auf außen- und innenpolitischer Ebene zukommt, wird im vorliegenden Kapitel genauer erklärt. Dabei wird zudem erläutert, inwiefern nicht nur die jeweilige inhaltliche Funktion des Proxys ein erklärungswürdiges Phänomen ist, sondern auch dessen institutionelle Anbindung.

Zunächst wird jedoch das Attributionsproblem als asymmetrische Interdependenzsituation behandelt und diskutiert, welche Rolle offensive und defensive Cyberproxys dabei für die jeweiligen Regimetypen spielen können. Darauf aufbauend werden im Anschluss die Variablen des Erklärungsmodells (Abbildung 8) aus Perspektive des neuen Liberalismus konzeptualisiert.

Abbildung 8: Liberales Erklärungsmodell staatlicher Cyberproxy-Strategien



(Eigene Darstellung)

3.1 *Why Cyberproxys Matter:* Das Attributionsproblem als asymmetrische Interdependenzsituation

Besonders im Cyberspace müssen bei der Entscheidung einer Regierung, ob und wie eine Attribution vorgenommen wird, die potenziellen Folgen der Handlung bereits mitgedacht werden. Auch wenn dem Opfer in vielen Fällen der jeweilige Urheber wohl bekannt sein dürfte, bedingen die aufgezeigten Interdependenzen auf allen drei Liberalismusebenen die vermutete Zurückhaltung vor allem demokratischer Regierungen, das Attributionsproblem als Problem der völkerrechtlichen Verantwortungsverregelung und weniger der -identifizierung zu adressieren.[1]

Aus autokratischer Sicht vereinfacht das Internet das Durchführen disruptiver Konfliktmaßnahmen unterhalb der kritischen Gewaltschwelle. Da diese technischen Möglichkeiten bei Zielen mit entsprechenden Attributionskapazitäten jedoch nicht zwingend ausreichen, um eine Identifizierung als Täter zu vermeiden, gilt es, die Bedingungen für demokratische Attributionen zu erschweren bzw. die Kosten hierfür im Rahmen der Interdependenzbeziehung in die Höhe zu treiben. Konkret bedeutet dies, die Rationalitätsgrundlage demokratischen Handelns in Folge einer Cyberoperation durch die (oftmals ambivalente) Kreierung einer Plausible Deniability zu manipulieren.[2] Die Demokratien zur Verfügung stehenden Information sollen dergestalt

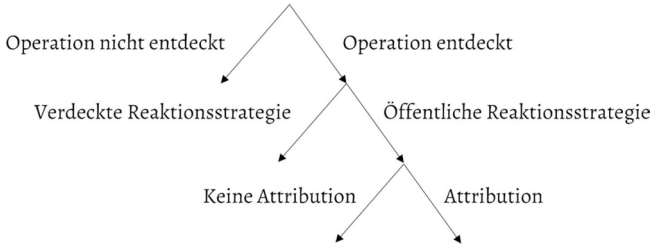
1 Experteninterview mit Dr. Brandon Valeriano, Mitglied der US-Cyber-Solarium-Commission, am 28.09.2020.

2 Inwiefern hierbei eher von einer »Implausible Deniability« gesprochen werden sollte, also einer »apparent, but unacknowledged action«, wird besonders für die öffentlichkeitswirksameren russischen Cyberproxy-Operationen von Bedeutung sein. So argumentieren Cormac und Aldrich, dass nur solche Operationen eine *plausibel* abstreitbare *verdeckte* Operation seien, die »neither acknowledged nor apparent« sind, was somit bewusst öffentlich stattfindende Operationen ausklammern

beschränkt bzw. beeinflusst werden, dass diese vor einer direktstaatlichen Attribution zurückschrecken, mit dem Wissen, dass eine Reaktion in Folge einer stets möglichen Fehlattribution potenziell schwere Folgen haben könnte. Der Einsatz von Proxys ist dafür ein geeignetes Mittel, da durch die hiermit geschaffene Informationsasymmetrie die Präsentation umfassender Beweise im Sinne der ›True Attribution‹ sowie die auf rechtstaatlichen Prinzipien basierende Adressierung solcher indirekten Cyberangriffe für demokratische Regierungen erschwert werden. Lässt sich eine staatliche Involvierung lediglich vermuten, jedoch rechtlich nicht einwandfrei belegen, sind die Kosten für eine dennoch erfolgende politische Attribution seitens der Demokratie in Richtung der Autokratie erhöht (Egloff 2020a, S. 61–62). Zudem könnte eine eskalative Reaktion die eigene Verwundbarkeit im Rahmen dieser Interdependenzsituation nicht wie geplant reduzieren, sondern weiter erhöhen. Somit stellte bislang aus autokratischer Sicht das Verbleiben unterhalb der kritischen Gewaltschwelle im Cyberspace eine Art Versicherung dar, die es erlaubte, mithilfe von Cyberoperationen negativ asymmetrische Interdependenzverhältnisse gegenüber Demokratien in der konventionellen Sphäre zu manipulieren (vgl. Tsygankov 2019, S. 164). Zusammenfassend kann somit konstatiert werden, dass Autokratien ihre geringere Vulnerabilität im Rahmen der asymmetrischen Attributionsinterdependenzsituation instrumentalisieren, um mithilfe von Proxys ihre höhere Verwundbarkeit in anderen Interdependenzbeziehungen zu verringern (Vulnerabilitäts-Linkage).

Aus demokratischer Perspektive ist nicht die Täterbeschreibung autokratischer ›Cyber-Rogue-States‹ per se das Problem, sondern die Entscheidung, ob dies öffentlich kommuniziert wird und wie entsprechend im weiteren Verlauf darauf reagiert werden soll (s. Abbildung 9).

Abbildung 9: Die Strategiewahl der Opfer von Cyberoperationen



(Eigene Darstellung basierend auf Baram und Sommer 2019, S. 202)

würde (2018, S. 482). Laut Carson und Yarhi-Milo nutzen Staaten zudem »covert action to convey intentions and coerce adversaries« (2017, S. 124), was besonders für den offensiven Proxy-Gebrauch autokratischer Staaten von Relevanz sein könnte. Auf demokratischer Seite steht dagegen im Vordergrund, inwiefern die angestrebte Geheimhaltung geheimdienstlicher Quellen die defensive Cyberproxy-Beziehung mit beeinflussen, im Rahmen sogenannter »Disclosure Dilemmas« (vgl. Carnegie und Carson 2020).

Wird eine öffentliche Attribution als verbale Eskalation verstanden (Steffens 2018, S. 143), könnten hierdurch auch auf der konventionellen Ebene Konflikteskalationen herbeigeführt werden. Alternativ wären die Effizienz sowie die rechtsstaatliche Integrität potenzieller Gegenmaßnahmen nur eingeschränkt gegeben, weshalb Demokratien bisher oftmals der »*tacit collusion*« (Egloff 2020b, S. 487) im Falle verdeckter Cyberoperationen den Vorzug gaben. Im Gegensatz zu ihren autokratischen Pendants erfordert der breitere Herrschaftszugang einer großen Anzahl an gesellschaftlichen Akteursgruppierungen, dass sich deren Interessen auch in der jeweiligen Außenpolitik der Demokratie widerspiegeln, um die Wiederwahl der Regierung nicht in Gefahr zu bringen. Scheitert nun aber eine demokratische Regierung bei der Beantwortung einer autokratischen Cyberaggression, etwa indem ihre Handlungen folgenlos bleiben und die Cyberangriffe ungehindert fortgeführt werden oder die demokratische Reaktion zu noch größeren Kosten für die eigene Bevölkerung führt, bestünden begründete Anreize für die Regierung, eine politische Attribution in Zukunft zu vermeiden und politischem Handlungsdruck somit aus dem Weg zu gehen. Das asymmetrische Interdependenzverhältnis besteht hierbei somit im Rahmen der Attributionsproblematik zwischen der demokratischen Regierung sowie den gesellschaftlichen Interessensgruppen mit einem Mindestmaß an Zugang zum politischen System, zumeist bereits gewährleistet durch das Wahlrecht. Ausgelöst wird die Salienz dieses Verhältnisses erst durch die offensive Cyberproxy-Nutzung autokratischer Staaten, die die asymmetrische Vulnerabilität demokratischer Regierungen auf republikanischer Ebene ausnutzen und teilweise auch offenlegen.

Der inklusivere Herrschaftszugang domestischer AkteurInnen in demokratischen Systemen, gepaart mit deren Interessen im Hinblick auf eine effiziente Beantwortung ausländischer Cyberoperationen, bedingt aus demokratischer Sicht die Konstitution des Attributionsproblems als asymmetrische Interdependenzkonstellation nach innen und außen. Trotz der beschriebenen Vorbehalte vor einer Konflikteskalation in Folge einer Attribution verlangen die Interessensdurchsetzungschancen domestischer AkteurInnen, dass auf Cyberoperationen reagiert werden *muss*, sofern diese öffentlich bekannt geworden sind. Defensive Cyberproxys können demokratischen Regierungen dabei helfen, dieses Dilemma aufzulösen, indem *sie* Attributionen vornehmen.[3] Somit wird die Informationsmanipulation durch den autokratischen Proxy-Einsatz zumindest stellvertretend in ihrer Wirkung reduziert, ohne dabei jedoch Gefahr zu laufen, unter öffentlichen Reaktionsdruck zu geraten und somit in einer Situation mit potenziell unvollständiger Information nur begrenzt rational handeln zu können. Dies könnte die Verwundbarkeit innerhalb dieser Interdependenzbeziehung sowohl gegenüber dem autokratischen Angreifer als auch gegenüber domestischen Interessensgruppen reduzieren. Der Einsatz autokratischer und demokratischer Cyberproxys im Rahmen des Attributionsinterdependenzverhältnisses ist somit bislang gegenseitig bedingt: Solange Autokratien mit ihren Cyberproxys die kritische Gewaltschwelle nicht überschreiten, verfügen Demokratien bislang auch über den notwendigen domestischen Spielraum, um ihrerseits durch den Einsatz defensiver Cyberproxys auf eine mögliche Konflikteskalation zu verzichten, frei nach dem Motto: »*Attribution is what states make of it*« (Rid

3 Dieses lässt sich auch als das Dilemma der »*Symmetrierung der Kampfstrategie vs. Asymmetrierung der Legitimität*« beschreiben (Wassermann 2014, S. 266).

und Buchanan 2015, S. 4). Dennoch liegt der Fokus der vorliegenden Arbeit in erster Linie auf dem Entstehen demokratischer und autokratischer Cyberproxy-Strategien auf Grundlage domestischer Präferenzkonstellationen. Interaktionistische Effekte im Sinne einer Tit-for-Tat-Logik können in diesem Rahmen lediglich angedeutet werden, sollten jedoch in weiteren Forschungsvorhaben expliziter im Fokus stehen, etwa im Rahmen zu identifizierender Cyberkonfliktzyklen.

3.2 Funktion und Art der Cyberproxys: Wer macht was?

Als abhängige Variable fungieren sowohl auf autokratischer als auch demokratischer Seite die beiden Aspekte der Funktion (AV I) und Art (AV II) der jeweiligen Cyberproxys. Durch diese Unterscheidung kann der Einfluss verschiedener Vulnerabilitätsasymmetrien auf ideeller, wirtschaftlicher sowie republikanischer Ebene genauer untersucht werden.

3.2.1 Funktion und Art autokratischer Cyberproxys

Es werden folgende Funktionen (AV I) autokratischer Cyberproxy-Nutzungen unterschieden, die teilweise mehrere Liberalismus-Ebenen betreffen:

Tabelle 1: Übersicht autokratischer Cyberproxy-Funktionen

<table>
<tr><th>Ideelle Ebene</th><th>Wirtschaftliche Ebene</th><th>Republikanische Ebene</th></tr>
<tr><td>Politische Cyberspionage</td><td>Ökonomische Cyberspionage</td><td>Überwachung Regimeeliten</td></tr>
<tr><td>Schwächung politischer Gegner (Staaten) ohne gewaltsamen konventionellen Konflikt</td><td>Militärtechnologische Cyberspionage</td><td rowspan="4">Überwachung Regimegegner (In- und Ausland)</td></tr>
<tr><td>Schwächung politischer Gegner (Staaten) mit gewaltsamem konventionellem Konflikt (auch durch strategisch-operative Unterstützung)</td><td rowspan="3">Strategisch-operative Unterstützung gewaltsamer konventioneller Konflikte</td></tr>
<tr><td>Schwächung demokratischer Institutionen/Werte</td></tr>
<tr><td>Überwachung Regimegegner</td></tr>
</table>

(Eigene Darstellung)

1. Manipulation asymmetrischer Verwundbarkeiten auf ideeller Ebene

Cyberproxys können auf unterschiedliche Weise asymmetrische Vulnerabilitäten hinsichtlich der ideellen Ebene manipulieren:

Politische Cyberspionage vs. andere Staaten
Indem eine Autokratie demokratische Staaten auch in Friedenszeiten ausspioniert, kann sie ihre Verhandlungsmacht vergrößern. Die gewonnenen Daten können dazu beitragen, die bislang größeren demokratischen Interessensdurchsetzungschancen auf internationaler Ebene zu reduzieren und somit zunehmend die eigenen ideellen Interessen in IOs durchzusetzen. Gleiches gilt auch für bilaterale Verhandlungen zwischen besagten Staaten. Ein ähnliches Vorgehen wäre jedoch auch gegenüber rivalisierenden benachbarten Autokratien plausibel.

Schwächung politischer GegnerInnen ohne zugrunde liegendem (gewaltsamem) konventionellem Konflikt
Handelt es sich beim Gegenüber um eine militärisch überlegene Demokratie, mit der aktuell kein gewaltsamer konventioneller Konflikt besteht, können Cyberproxy-Handlungen auf die Erosion demokratischer Normen und Werte sowie das Signalisieren demokratischer Ohnmacht gegenüber den autokratischen Cyberoperationen abzielen. In beiden Fällen ist das Ziel, die ideelle Einheit des demokratischen Gegenübers zu schwächen, indem versucht wird, Einfluss auf die sozialen Identitäten der Bevölkerung zu nehmen und relative Vorteile im Rahmen dieser Interdependenzbeziehung zu erzielen. Handelt es sich beim anvisierten Staat stattdessen um eine militärisch maximal ebenbürtige Autokratie, könnten die Cyberproxy-Handlungen noch disruptivere Formen annehmen und im extremsten Falle den Cyberkonflikt in die analoge Sphäre übertragen.

Schwächung politischer GegnerInnen mit zugrunde liegendem (gewaltsamem) konventionellem Konflikt
Befindet sich eine Autokratie bereits in einem gewaltsamen konventionellen Konflikt mit einer militärisch überlegenen Demokratie, könnten ihre Cyberproxy-Handlungen darauf abzielen, diese vor allem auf moralischer Ebene zu schwächen, ohne eine Konflikteskalation zu riskieren. Die Verwundbarkeiten des demokratischen Landes im Cyberraum könnten, bei gleichzeitig konventioneller Überlegenheit, das Pflichtgefühl sowie die Verbundenheit der demokratischen Bevölkerung gegenüber der eigenen Regierung sukzessive schwächen, sofern sie keinen Ausweg aus dieser Interdependenzvulnerabilität findet. Cyberproxy-Operationen, die direkte strategische oder operative Unterstützung für diesen allgemeinen Konflikt bieten, können ebenfalls der eigenen ideellen Präferenzdurchsetzung dienen.

Schwächung/Unterminierung demokratischer Institutionen/Werte
Mithilfe von Cyberproxys können autokratische Regierungen zudem gezielt demokratische Institutionen in ideeller Hinsicht angreifen und somit untermauern, warum es auch dreißig Jahre nach Ende des Kalten Krieges zu keinem »*Ende der Geschichte*« gekommen ist (Fukuyama 2006). Gleiches gilt für zivilgesellschaftliche AkteurInnen wie Non-Governmental Organizations (NGOs) oder auch JournalistInnen und Medien-VertreterInnen, die vor allem zum Ziel von informationsgesteuerten Operationsformen werden können.

Überwachung von Regime-GegnerInnen im In- und Ausland
Zuletzt zielt auch eine Überwachung von Regime-GegnerInnen auf eine Manipulation des bestehenden ideellen Interdependenzverhältnisses ab: Gelingt es diesen, entweder zu Hause oder im Ausland gegenüber einer liberal-demokratischen Audience ihre sozialen Identitäten in Abgrenzung zu jenen des autokratischen Regimes erfolgreich zu propagieren, erhöht sich deren Herrschaftszugang zumindest indirekt. Cyberoperationen können autokratischen Regimen demnach dabei helfen, diese antizipierte Regimegefahr auf ideeller Ebene zu erkennen und zu entschärfen.[4]

2. Manipulation asymmetrischer Verwundbarkeiten auf wirtschaftlicher Ebene

Als zweite autokratische Cyberproxy-Funktion wird deren Wirken auf wirtschaftliche Interdependenzverhältnisse diskutiert:

Ökonomisch motivierte Cyberspionage
Wirtschaftsspionage kann die autokratische Abhängigkeit von ökonomisch führenden Demokratien reduzieren. Cyberproxys verringern die stärkere Vulnerabilität der meisten Autokratien auf wirtschaftlicher Ebene und schützen zugleich vor demokratischen Liberalisierungsforderungen, indem sie potenzielles ›Leapfrogging‹ ermöglichen. Somit können die wirtschaftlichen Präferenzordnungen gegenüber Demokratien trotz bestehender Inkompatibilitäten auf dieser sowie den anderen beiden Ebenen durchgesetzt werden. Gleichzeitig können domestische Output-Legitimationserfordernisse bedient werden, ohne etwas an der eigenen wirtschaftlichen Präferenzordnung ändern zu müssen (Mischung aus kommerziellem und republikanischem Argument).

Militärtechnologisch motivierte Cyberspionage
Hinsichtlich technologischer Entwicklungen argumentiert der republikanische Liberalismus, dass die demokratische Verfasstheit eines Staates im Gegensatz zum autokratischen Institutionenarrangement wirtschaftliche Innovationen grundlegend begünstigt, weil dessen Institutionen auf die legitime und inklusive Verteilung kollektiver Güter ausgerichtet sind (Moravcsik 1997, S. 531). Aufgrund der oftmals unklaren Unterscheidung zwischen ökonomisch und sicherheitspolitisch motivierter Cyberspionage wird daher auch der Diebstahl militärtechnologischer Daten als Mittel angesehen, um wirtschaftliche Abhängigkeitsverhältnisse gegenüber Demokratien auch im militärtechnologischen Bereich zu manipulieren.

Strategisch-operative Unterstützungsleistung im Rahmen eines konventionellen Konfliktes
Zuletzt besitzen auch gewaltsame konventionelle Konflikte oftmals erhebliche Implikationen für wirtschaftliche Interdependenzverhältnisse zwischen den beteiligten Staaten. Geht es beispielsweise um die Eroberung rohstoffreicher Gebiete oder für den Han-

4 Im Rahmen sog. »*Tainted Leaks*« können nach vorheriger Manipulation sensible Daten der anvisierten AkteurInnen veröffentlicht und deren Interessensdurchsetzungschancen somit geschwächt werden (Hulcoop et al. 2017).

del strategisch bedeutsamer Infrastrukturen, könnten Cyberproxys den konventionellen Streitkräften einer Autokratie in ihren militärischen Bemühungen behilflich sein. Dabei ist jedoch entsprechend dem bisherigen Forschungsstand eher von einer Substitutionswirkung auszugehen.

3. Manipulation asymmetrischer Vulnerabilitäten auf republikanischer Ebene

Cyberproxys erfüllen für autokratische Regierungen jedoch auch auf domestischer Ebene wichtige Funktionen, indem Asymmetrien im Herrschaftszugang bzw. der Interessens-durchsetzungschancen manipuliert werden können:

Überwachung/Kontrolle potenziell regimegefährdender Elitengruppierungen
Unabhängig von der Tätigkeit ist mit dem bloßen Einsatz sowie der jeweiligen institutionellen Anbindung eines Proxys eine Proxy-Funktion auf republikanischer Ebene verbunden: Durch die Beschränkung oder Erweiterung des Herrschaftszugangs bestimmter Elitengruppierungen deren Coup-Proofing-Potenzial auszubalancieren. Die republikanisch-liberalen Herrschaftserfordernisse autokratischer Systeme führen zum Gebrauch unterschiedlicher Cyberproxys. Indem kontextabhängig etwa das Militär die Kontrolle über die staatlichen APTs hat, zu anderen Zeiten jedoch der zivile Geheimdienst, kann eine autokratische Regierung entsprechend antizipierter Asymmetrien im Interdependenzverhältnis gegenüber diesen Gruppen auf republikanischer Ebene reagieren und somit einer zu starken Ermächtigung dieser Elitengruppierungen im Cyberspace vorbeugen. Gleichzeitig ermöglicht eine strengere staatliche Kontrolle der Proxys, dass auch diese ihre potenziellen Eigeninteressen nicht zu autonom im Cyberspace verfolgen können.

Überwachung von Regime-GegnerInnen im In- und Ausland
Neben den AkteurInnen der Winning Coalition stellt jedoch auch das breite Volk eine potenzielle Coup-Gefahr für autokratische Regime dar. Cyberproxys könnten dabei helfen, potenzielle Regime-GegnerInnen innerhalb der Bevölkerung im In- und Ausland zu erkennen und autokratische Informationsdefizite aufgrund des verkürzten/dysfunktionalen Transmissionsriemens auszugleichen. So soll verhindert werden, dass diese Druck auf Teile der Winning Coalition ausüben und deren Präferenzen zu Ungunsten der Regierung verändern. Mit dem Cyberproxyeinsatz wird hier das Ziel verfolgt, die Interessensdurchsetzungschancen der Regime-GegnerInnen zu verringern und die bestehende Asymmetrie auf republikanischer Ebene aus Sicht des Regimes weiterhin positiv zu gestalten.

Hinsichtlich der AV II, der Art der Proxys, steht in erster Linie die institutionelle Anbindung der in der Stellvertreterrolle agierenden AkteurInnen im Vordergrund. Zu deren Ausdifferenzierung wird auf die bestehende Forschungsliteratur zu nichtstaatlichen AngreiferInnen im Cyberspace rekurriert, die in Kapitel 1.2 vorgestellt wurde. Somit werden in erster Linie folgende Akteursgruppen als potenzielle Cyberproxy-Rollenträger konzeptualisiert:

- Cybermilizen,
- patriotische HackerInnen,
- Cyberkriminelle,
- PMSCs sowie
- nationale Forschungseinrichtungen/nationale Technologiefirmen.[5]

Die Art des Proxys kann gleichzeitig Hinweise darauf geben, wie umfassend die staatliche Verantwortlichkeit bei den jeweiligen Operationen einzuschätzen ist. Auch wenn der HD-CY.CON lediglich zwischen staatlichen, privaten und staatlich gesponserten CyberakteurInnen unterscheidet und für die oben genannte Kategorisierung die Quellen der als ›state-sponsored‹ kodierten Fälle nochmals analysiert werden müssen, soll in den Fallstudien (wenn möglich) unterschieden werden, ob bei einer Cyberproxy-Aktion der attribuierte Sponsor durch die Duldung der Proxy-Handlungen,[6] deren materielle Unterstützung oder die organisatorische Anleitung und Kontrolle in Erscheinung trat (vgl. Rivera 2015, S. 15).[7] Ein potenzieller Wandel hierbei könnte auch Aufschluss darüber geben, ob eine Autokratie ihre Proxys nach anfänglicher Distanz in Folge veränderter Attributionspraktiken demokratischer Länder nun unter zentralerer Kontrolle hält (vgl. Canfil 2020). Wichtig ist dabei im Hinblick auf die Konzeptualisierung der letztgenannten Funktionen auf republikanischer Ebene, ob sich Hinweise darauf finden lassen, welche AkteurInnen/Behörden im autokratischen System bei den jeweiligen Proxy-Operationen als staatliches Bindeglied fungierten. Dies könnte ein Indikator dafür sein, dass deren Interessensdurchsetzungschancen seitens des Regimes als potenziell ungefährlicher eingeschätzt wurden, oder aber, dass diese zum jeweiligen Zeitpunkt stärker ausgeprägt waren.

3.2.2 Funktion und Art demokratischer Cyberproxys

Für demokratische Cyberproxys wird eine weniger strikte Trennung zwischen den beiden AVs angenommen. Vielmehr ergibt sich bei diesen aus der angestrebten Funktion des Proxys auch notwendigerweise dessen Art, da das Spektrum an potenziellen AkteurInnen, die die jeweilige Handlung ausführen könnten, exklusiver ist als im Falle offensiver Cyberoperationen. Die nachfolgend aufgelisteten Funktionen werden somit priva-

5 Die bisherige Cyberproxy-Forschung behandelte diese bislang noch nicht als relevante AkteurInnen. Gerade wirtschaftlich stark nach Modernisierung strebende Autokratien könnten jedoch bei der Vorbereitung und Ausführung ihrer Cyberangriffe gezielt auf die Kenntnisse und Ressourcen nationaler Universitäten, Forschungsinstitutionen sowie staatlicher oder halbstaatlicher IT-Unternehmen zurückgreifen.

6 Für die Kategorie der Proxy-Duldung ist jedoch anzumerken, dass diese voraussichtlich am seltensten auch als Proxy-Operation attribuiert wird, aufgrund der nochmal sehr viel schwerer nachweisbaren Verletzung der ›Due Diligence‹ seitens eines autokratischen Staates. Die Ransomware-Operationen in den USA Mitte 2021 u.a. gegen die Firma Colonial Pipeline, könnten jedoch längerfristig zu einer stärkeren Adressierung dieser Sorgfaltsverantwortung seitens demokratischer Opferstaaten führen, wie es die Reaktion der US-Administration zumindest andeutete (Jasper 2021).

7 Im Abschnitt über die Operationalisierung der autokratischen AVs (Kapitel 4.4.2) wird hierzu das in der Cyberkonfliktforschung bekannte ›Spektrum staatlicher Verantwortlichkeit‹ von Jason Healey 2011 vorgestellt.

ten AkteurInnen, in erster Linie IT-Firmen, mit eigenen Threat-Research-Forschungseinheiten zugesprochen.[8] Als konstante Teilfunktion privater IT-Attributionen fungiert auf allen drei Ebenen deren Legitimationsfunktion hinsichtlich nachgelagert stattfindender politischer Attributionen.

Tabelle 2: Übersicht demokratischer Cyberproxy-Funktionen

Ideelle Ebene	Wirtschaftliche Ebene	Republikanische Ebene
Steigerung der soziopolitischen Resilienz	Steigerung der technischen Resilienz	Reduzierung des politischen Handlungsdrucks/Signaling (dauerhaft vs. temporär) bzw. Erweiterung des politischen Handlungsspielraums
Schaffung von Legitimation politischer Attributionen	Schaffung von Legitimation politischer Attributionen	Schaffung von Legitimation politischer Attributionen

(Eigene Darstellung)

1. Manipulation asymmetrischer Verwundbarkeiten auf ideeller Ebene

Stellvertretende Attributionen seitens nichtstaatlicher AkteurInnen können für demokratische Regierungen auf unterschiedliche Weise ideelle Verwundbarkeitsasymmetrien auf außenpolitischer oder domestischer Ebene manipulieren:

Reduzierung der ideellen Verwundbarkeiten gegenüber autokratischen Cyberoperationen (soziopolitische Resilienz)
Indem private AkteurInnen autokratische CyberangreiferInnen als solche benennen, lenken sie den Fokus der demokratischen Öffentlichkeit auf die Unvereinbarkeit solcher Handlungen mit den eigenen sozialen Identitäten. Somit kann zumindest teilweise der

8 An dieser Stelle könnte eingewandt werden, dass auch Medien potenziell als Attributions-Proxies fungieren könnten und dies vielleicht auch aufgrund teilweise staatlichen Interesses an dem Leaken von »*classified information*« tun (Pozen 2013). Der HD-CY.CON-Datensatz ist durch die Kategorie der ›Media-based Attribution‹ im Stande, auch dieses potenzielle Durchstechen von Infos an die Presse zu erfassen. Wenn die Quelle jedoch als ›Government Official‹ benannt wird, kann zwar von einem Durchstechen der Attribution, jedoch nicht von einer Verschleierung dieser Praxis gesprochen werden. Im Sinne der Proxy-Logik wird bei Medien zudem davon ausgegangen, dass das Veröffentlichen von Informationen der Kern ihrer Tätigkeit ist, unabhängig davon, ob dies im Interesse oder gegen den Willen der jeweiligen Regierung geschieht, was natürlich auch bei IT-Unternehmen durchaus der Fall sein kann. Jedoch wird die ›vierte Gewalt‹ wenn überhaupt, dann als institutionalisierter Proxy angesehen, da hier der oftmals typische ad-hoc-Charakter eines Proxys fehlen würde. IT-Unternehmen entwickelten erst im Laufe der Jahre eigene Attributionskapazitäten und Aktivitäten, da dies nicht von Anfang an zu ihren Tätigkeitsfeldern gehörte. Zudem gibt es auch immer noch genug Firmen, die überhaupt keine Attributionen vornehmen.

auf ideeller Ebene intendierte disruptive Effekt der Cyberhandlungen reduziert werden. Ziel dabei ist es, die Verbundenheit des demokratischen Volkes gegenüber der eigenen Regierung trotz deren potenzieller Passivität in Folge der Cyberoperation nicht schwächer werden zu lassen. Private Cyberattributionen können somit aus demokratischer Sicht die Sensitivität auf ideeller Ebene in solchen Fällen zumindest reduzieren, für den Fall, dass die demokratische Regierung keine geeigneten Maßnahmen zur Reduzierung der Vulnerabilität ergreifen kann oder will. Schafft es eine Autokratie mithilfe ihrer Cyberproxys, unterschiedliche soziale Identitäten innerhalb eines demokratischen Landes gezielt auszunutzen bzw. weiter zu polarisieren, kann diese Inkompatibilität den Handlungsspielraum demokratischer Regierungen nach innen und außen in der Folge weiter einschränken. Darüber hinaus können technische Berichte von IT-Firmen auch direkt die Resilienz demokratischer Bevölkerungen gegenüber autokratischen Cyberoperationen stärken, indem das hierfür notwendige Problembewusstsein geschaffen wird.

2. Manipulation asymmetrischer Vulnerabilitäten auf wirtschaftlicher Ebene

Die oben beschriebenen Dynamiken lassen sich ebenfalls auf autokratische Cyberoperationen mit wirtschaftlicher Zielsetzung anwenden:

Reduzierung der wirtschaftlichen Verwundbarkeiten gegenüber autokratischen Cyberoperationen (technische Resilienz)
Da etwa in liberalen Demokratien zumeist der Kapitalismus als dominantes Wirtschaftssystem Teil der sozialen Identitäten des Landes ist, lassen sich die ideelle und wirtschaftliche Ebene an dieser Stelle nicht gänzlich voneinander trennen. Indem in Folge wirtschaftlicher Cyberspionage private AkteurInnen Attributionen in Richtung autokratischer CyberangreiferInnen vornehmen, lässt sich die Cyberspionage als Angriff auf das demokratische Wirtschaftssystem und einen wichtigen Teil sozialer Identitäten darstellen. So kann der Fokus von der eigenen Verwundbarkeit auf wirtschaftlicher Ebene auf das aus ideeller Sicht zu verurteilende Handeln autokratischer Staaten verschoben werden.

Noch wichtiger ist jedoch die Präventivfunktion technischer IT-Berichte: Indem in diesen autokratische ›Techniques, Tactics and Procedures‹ (TTPs) im Cyberraum offengelegt und vor allem an wirtschaftliche AkteurInnen als Hauptadressaten vermittelt werden, kann diese stellvertretende Attribution durch ihre technische Fundiertheit bestehende Vulnerabilitäten einer Demokratie reduzieren.

3. Manipulation asymmetrischer Verwundbarkeiten auf republikanischer Ebene

Auch defensive Cyberproxys können für demokratische Regierungen gegenüber der domestischen Audience eine bedeutende Funktion auf republikanischer Ebene erfüllen:

Manipulation asymmetrischer Verwundbarkeiten auf republikanischer Ebene (Reduzierung politischen Handlungsdrucks/Signaling)
Demokratische Regierungen können defensive Cyberproxys nutzen, um ihre im Ver-

gleich zu Autokratien stärkere Vulnerabilität gegenüber einer Vielzahl an domestischen AkteurInnen auf republikanischer Ebene zu manipulieren.[9] Dies kann auch das Ausbalancieren der Interdependenzen der Regierung mit der eigenen Geheimdienstcommunity, der politischen Opposition oder KritikerInnen der eigenen Partei bedeuten. Geheimdienste sind oftmals Vetospieler öffentlicher Attributionen, da sie fürchten, hierdurch einen Teil ihrer Attributionsvektoren durch deren Offenlegung zu ›verlieren‹. Die Opposition oder andere, nicht in der Regierung vertretene AkteurInnen des politischen Systems sowie der Bevölkerung, haben gleichzeitig jedoch oftmals ein Interesse an öffentlicher Attribution. Somit können defensive Cyberproxys das aufgezeigte Handlungsdilemma für demokratische Regierungen zumindest reduzieren. Indem der Proxy eine öffentliche Attribution vornimmt, kann dem Angreifer sowie der Öffentlichkeit signalisiert werden, dass der Täter bekannt ist. Gleichzeitig gerät die Regierung selbst jedoch nicht unter ähnlichen Handlungsdruck wie im Falle einer eigenen Attribution und muss keine Attributionskapazitäten der Geheimdienste offenlegen.[10]

Hinsichtlich der AV II, der Art der demokratischen Cyberproxys, wird in dieser Arbeit argumentiert, dass eine Lücke zwischen primär technischer sowie politischer Attribution existiert, weshalb Firmen aus dem IT-Bereich bzw. potenziell auch frei arbeitende IT-ExpertInnen mit entsprechenden technischen Fähigkeiten als relevante Proxys konzeptualisiert werden müssen. Eine weitere Spezifizierung dabei lautet, dass hauptsächlich nationale IT-Firmen, die in dieser Rolle für ein demokratisches Land agieren, als Proxys konzeptualisiert werden.[11] Aufgrund des besonderen Delegationsmodus dieser Proxy-Nutzungen könnte bei fehlenden nationalen Ressourcen nicht einfach wie im Falle von ›Hacking-for-Hire‹-Prozessen auf ausländische AkteurInnen ausgewichen werden. Dass demokratische Regierungen ausländischen IT-Firmen oder Internet-Service-Providern (ISPs) Geld oder Aussicht auf Regierungsaufträge für die jeweilige Proxy-Funktionserfüllung anbieten könnten, erscheint weniger plausibel als eine Fokussierung auf nationale AkteurInnen, sofern diese vorhanden sind. Ein Grund hierfür ist der öffentliche Charakter der Attribution als Proxy-Funktion. Der Stellvertreter kann nicht, wie bei offensiven Cyberoperationen, verdeckt operieren, da in diesem Handlungsfeld nicht die Handlung oder Urheberschaft, sondern die staatliche Verantwortlichkeit verschleiert werden soll.[12] Reichweite, Legitimität und Wirkung stellvertretender Attributionen

9 Interview mit einem leitenden Mitarbeiter eines deutschen Bundesministeriums, am 02.12.2020.

10 Inwiefern eine solche Verschleierungstaktik politischer Verantwortlichkeiten jedoch im Rahmen unterschiedlicher Kontexte als wahrscheinlicher gelten kann als in anderen, wird Gegenstand der Konzeptualisierungen der übrigen Variablen sein. Zudem könnte eine stellvertretende Attribution lediglich zeitlich begrenzt das Attributionsvakuum demokratischer Regierungen füllen, sowie nachgelagerten politischen Attribution mithilfe technischer Evidenzen die notwendige Legitimität verleihen.

11 Selbstverständlich können auch ausländische, international agierende Firmen eine stellvertretende Attribution vornehmen. Jedoch lässt sich bei diesen der Delegationscharakter schwerer plausibilisieren, als im Falle nationaler Unternehmen, die ideelle, ökonomische, rechtliche und manchmal sogar politische sowie personelle Interdependenzen zu ihren jeweiligen Regierungen aufweisen.

12 Anders formuliert will die demokratische Regierung verschleiern, dass ihre Informationslage eine eigene Attribution sehr wohl zulassen würde, die es jedoch aufgrund möglicher Fehlschlüsse,

dürften bei nationalen IT-Firmen weitaus größer eingestuft werden als bei ausländischen VertreterInnen. Ein weiterer wichtiger Grund besteht in den immateriellen und materiellen Anreizstrukturen, die seitens einer Regierung für Firmen innerhalb der nationalen Rechtsprechung ausgeprägter sein dürften als für ausländische Unternehmen.

3.3 Gesellschaftliche Präferenzkonstellationen als unabhängige Variable

Entsprechend der liberalen Theorieverortung stellen die jeweiligen gesellschaftlichen Präferenzen innerhalb autokratischer und demokratischer Staaten sowie deren Kompatibilität zueinander die Haupterklärungsvariable staatlicher Cyberproxy-Strategien dar. Aufgrund der daraus resultierenden Verwundbarkeitsasymmetrien entscheiden diese darüber, ob und wie beide Regimetypen die genannten Proxy-Funktionen bedienen wollen.

3.3.1 Autokratien

Unabhängig von den notwendigen technischen Voraussetzungen bedarf es konfliktiver Präferenzkonstellationen auf ideeller, wirtschaftlicher oder republikanischer Ebene zwischen einer Autokratie und anderen Staaten, damit Cyberoperationen im Allgemeinen und deren Durchführung mithilfe von Proxys im Besonderen für die Autokratie von Interesse sind. Dies ist der Fall, sobald Proxys entweder die eigenen Verwundbarkeiten innerhalb dieser Interdependenz verringern oder die Verwundbarkeiten des Gegenübers verstärken/ausnutzen sollen. In beiden Fällen ist die Wirkung eigener oder fremder Verwundbarkeitsasymmetrien zentral. Die erste Hypothese lautet daher:

> *H1: Je größer die eigene Verwundbarkeit im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen ist, desto größer sind die autokratischen Anreize für die Nutzung offensiver Cyberproxys.*

Grundlegend besitzen Autokratien auch untereinander konfliktive Präferenzkonstellationen. Verantwortlich hierfür können gegenseitig kostenverursachende domestische Präferenzen auf ideeller oder wirtschaftlicher Ebene sein, die vor allem auch zwischen unterschiedlichen Subtypen stärker ausgeprägt sein können. Zugleich könnte der dominante Herrschaftszugang einer bestimmten Elitengruppierung in einem autokratischen Subtyp die Interessensdurchsetzungschancen eines anderen einschränken, wodurch auch auf republikanischer Ebene intra-autokratische Varianzen zum Tragen kommen können. Der autokratische Subregimetyp kann somit als Teil des Ausdrucks der domestischen Präferenzkonstellation angesehen werden, der sich in erster Linie auf republikanischer Ebene niederschlägt. Daher beeinflusst er als Bestandteil der UV implizit mit, in welchem Ausmaß die beschriebenen Präferenzkonstellationen auf ideeller und kommerzieller Ebene erst entstehen können.

---

geheim zu haltender Geheimdienstmethoden, sowie oftmals fehlender Reaktionsoptionen zu verhindern gilt.

Prinzipiell können Präferenzinkompatibilitäten, die zugleich mit asymmetrisch verteilten Kosten im Rahmen einer wahrgenommenen Interdependenzbeziehung einhergehen, jedoch häufiger zwischen Autokratien und Demokratien vermutet werden, da zwischen den beiden Hauptregimetypen auf allen drei Liberalismus-Ebenen die größten grundlegenden Unterschiede bestehen. Die zweite Hypothese in Bezug auf autokratische Cyberproxy-Strategien lautet somit:

> *H2: Je stärker aufgrund konfliktiver Präferenzkonstellationen Regimetypenunterschiede in asymmetrischen Verwundbarkeiten resultieren, desto stärker sind die autokratischen Anreize für eine offensive Cyberproxy-Nutzung dem jeweiligen Staat gegenüber.*

Der dritte Zusammenhang zwischen UV und AVs verweist nochmals auf die Ausdifferenzierung letzterer: So resultieren die inhaltliche Funktion eines offensiven Cyberproxys, die Form und das Zielprofil der von ihm ausgeführten Cyberoperationen direkt aus der Ausgestaltung der hierfür maßgeblichen Verwundbarkeitsasymmetrie, basierend auf der Präferenzkonstellation zwischen den Staaten. Zwei Beispiele verdeutlichen diese Annahme: Eine Autokratie kann sowohl gegenüber anderen Autokratien als auch gegenüber Demokratien inkompatible Präferenzkonstellationen auf ideeller Ebene aufweisen. In beiden Szenarien ist für die Auswahl der jeweiligen Cyberoperationsform entscheidend, durch welche die angestrebte Manipulation der bestehenden Verwundbarkeitsasymmetrie am ehesten erreicht werden kann. Grundlegend erscheinen informationsbasierte Operationsformen wie Hack-and-Leak-Operationen hierfür geeigneter als verdeckt angelegte Cyberspionage-Operationen. Dieselbe Logik kann auf Präferenzinkompatibilitäten zwischen Autokratien und anderen Staaten auf wirtschaftlicher Ebene angewendet werden: Hierbei können Cyberspionage-Operationen mit dem Ziel, die wirtschaftlichen Informationsasymmetrien im Technologie-Bereich zum eigenen Vorteil zu manipulieren, als prinzipiell vorteilhafter eingestuft werden als etwa disruptive Cyberoperationen auf kritische Infrastrukturen.[13] Diese exemplarischen Ausführungen resultieren in folgender, dritter Hypothese:

> *H3: Je größer der erwartete Nutzen bestimmter Formen offensiver Cyberproxy-Operationen zur Reduzierung eigener Verwundbarkeiten auf ideeller und/oder wirtschaftlicher Ebene ist, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Autokratie.*

Zuletzt werden hinsichtlich des Wirkens der republikanischen Ebene auf die Art und institutionelle Anbindung autokratischer Cyberproxys (AV II) die innerautokratischen Präferenzkonstellationen betrachtet. Diesen wird ein direkter Einfluss darauf unterstellt, welche AkteurInnen eine autokratische Regierung als offensive Proxys in Betracht zieht und durch welche Elitengruppierungen deren Kontrolle/Leitung erfolgt:

---

13 Inkompatibilitäten zwischen Autokratien und Demokratien auf wirtschaftlicher Ebene können zudem Ausdruck oder auch Auslöser gleichzeitiger Interessenskonflikte auf ideeller Ebene sein. Wie bereits erwähnt, beziehen sich die sozialen Identitäten domestischer Akteursgruppen auch auf die jeweiligen Vorstellungen legitimer Verteilung öffentlicher Güter, mit somit direkten Implikationen für den wirtschaftlichen Bereich.

H4: Je größer die domestischen Verwundbarkeiten autokratischer Regierungen auf republikanischer Ebene aufgrund inkompatibler Präferenzkonstellationen sind, desto eher sind die Auswahl und institutionelle Anbindung der Proxys auch auf deren Manipulation ausgerichtet.

Gegenüber der eigenen Winning Coalition könnte dies bedeuten, dass ein autokratisches Regime die Kontrolle über seine Cyberproxys gezielt einer gewissen Akteursgruppe *nicht* anvertraut, sofern diese zum Regime inkompatible Präferenzen aufweist und somit im Cyberspace nicht noch stärker ermächtigt werden soll. Da jedoch neben Putschversuchen der Winning Coalition auch von unten entstehende Protestbewegungen breiterer Teile der Bevölkerung einem autokratischen Regime trotz Repressionsmaßnahmen gefährlich werden können, könnte dies eine engere Kontrolle nichtstaatlicher Cyberproxys oder die Instrumentalisierung im Ausland stationierter HackerInnen zur Folge haben.

3.3.2 Demokratien

Auf demokratischer Seite werden ebenfalls verschiedene Präferenzkonstellationen auf ideeller, wirtschaftlicher sowie republikanischer Ebene als Haupterklärungsvariable für die beschriebene defensive Cyberproxy-Nutzung konzeptualisiert. Sofern dabei vonseiten autokratischer Staaten die eigenen Verwundbarkeitsasymmetrien durch offensive Cyberoperationen regelmäßig ausgenutzt werden, sollten auch entsprechende Anreize für eine defensive Cyberproxy-Nutzung vorliegen. Das Konfliktpotenzial der domestischen Präferenzkonstellation im Verhältnis zu vor allem autokratischen Staaten beeinflusst somit wie auch im Falle der Autokratien die demokratische Cyberproxy-Nutzung:

H1: Je umfassender die eigenen Verwundbarkeiten im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen durch offensive Cyberoperationen ausgenutzt werden, desto größer sind die demokratischen Anreize für die Nutzung defensiver Cyberproxys.

Auch für demokratische Staaten gilt, dass diese sehr wohl auch untereinander konfliktive Präferenzkonstellationen auf einer oder mehreren der drei Liberalismus-Ebenen aufweisen können. So zeichnen sich liberale und illiberale Demokratien zwar durch die Gemeinsamkeit weitgehend freier und fairer Wahlen auf republikanischer Ebene aus, jedoch entwickeln sich letztere in den letzten Jahren zunehmend in Richtung elektoraler Autokratien, indem der Wahlprozess und dessen Integrität durch verschiedene AkteurInnen unterminiert werden (Levitsky und Ziblatt 2018). Hierfür werden vor allem Veränderungen der Präferenzkonstellationen auf der ideellen Ebene verantwortlich gemacht, die zwischen liberalen und illiberalen Demokratien potenziell auch zu steigenden Konfliktpotenzialen auf außenpolitischer Ebene führen können. Auch der demokratische Subtyp kann somit als Teil des Ausdrucks der domestischen Präferenzkonstellation angesehen werden und beeinflusst als Bestandteil der UV implizit mit, in welchem Ausmaß die beschriebenen Präferenzinkompatibilitäten auf ideeller, kommerzieller oder republikanischer Ebene erst entstehen können.

Nichtsdestotrotz wird auch bei Demokratien davon ausgegangen, dass die Verwundbarkeitsasymmetrie zwischen den beiden Regimetypenlagern größere Ausmaße annehmen dürfte als zwischen Demokratien untereinander, insbesondere im Cyberspace. So-

mit bestehen prinzipiell für Autokratien mehr Anreize und Möglichkeiten, Verwundbarkeiten demokratischer Länder im Cyberspace häufiger auszunutzen, da sie aufgrund der hier existierenden Asymmetrie regelmäßig im Vorteil sind.

Da, wie erwähnt, für demokratische Cyberproxys im Rahmen dieser Arbeit hinsichtlich der Art des Proxys eine geringere Varianz konzeptualisiert wird, bezieht sich die zweite Hypothese auf den Zusammenhang zwischen UV und AV I. Zwar wird grundlegend der stellvertretende Attributionsakt als defensive Funktion demokratischer Cyberproxys definiert, jedoch zeigte die Konzeptualisierung der AV I auch hier hinsichtlich über die bloße Verantwortungszuschreibung hinausgehender Funktionen technischer IT-Berichte eine gewisse Subvarianz auf. So können mit diesen technische Resilienzfunktionen bezüglich des Schließens von Sicherheitslücken oder einer allgemeinen Steigerung des Gefahrenbewusstseins besonders bedrohter Akteursgruppen verbunden sein. Als zweite Subfunktion wurde die Legitimation einer potenziell nachgelagerten, politischen Attribution benannt, die zum gleichen Attributionsschluss wie der technische Bericht kommt, hierfür jedoch aufgrund vorliegender Geheimhaltungserwägungen nicht die entsprechenden Evidenzen liefern kann. Welcher erweiterte Zweck mit einer gänzlich oder zeitlich begrenzten stellvertretenden Attribution für eine demokratische Regierung einhergehen kann, ist somit ebenfalls davon abhängig, inwiefern hierdurch die durch den Cyberangriff ausgenutzten bzw. offengelegten Verwundbarkeiten reduziert werden können.

> *H2: Je größer der erwartete Nutzen bestimmter Formen defensiver Cyberproxy-Operationen (Attributionen) zur Reduzierung eigener Verwundbarkeiten auf ideeller, wirtschaftlicher sowie republikanischer Ebene, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Demokratie.*

Ein Beispiel soll die hierbei angenommene Logik verdeutlichen: Erscheint es im Falle einer autokratischen Cyberoperation aus Sicht einer demokratischen Regierung ausreichend, die eigenen, technischen Verwundbarkeiten im Sinne einer Offenlegung der TTPs des Angreifers seitens eines defensiven Proxys zu stärken, ist eine nachgelagerte politische Reaktion unwahrscheinlicher. Wenn jedoch aufgrund des Profils und der Wirkweise der Operation bzw. aufgrund des Profils des Angreifers auch eine direkte, politische Signalwirkung ermöglicht werden soll, könnte die technische Attribution einer später erfolgenden politischen Attribution mehr Glaubwürdigkeit verleihen, vorausgesetzt, ihre Erkenntnisse deuten in dieselbe Richtung. Dasselbe gilt auch, falls der politische Handlungsdruck trotz erfolgter technischer Attribution so hoch ist, dass zu einem gewissen Zeitpunkt auch eine politische Attribution erfolgen *muss*.

3.4 Die nationale Cyberakteursumwelt als konditionierende Variable

Als konditionierende Variable wird in dieser Arbeit die nationale Cyberakteursumwelt konzeptualisiert. Dieser Begriff bedarf genauerer Spezifizierung: Unabhängig von der inhaltlichen Ausgestaltung der domestischen Präferenzordnungen bedingen die Existenz und Diversität staatlicher sowie nichtstaatlicher AkteurInnen, die im oder den Cyberspace betreffend aktiv sind, in welchem Umfang Autokratien oder Demokratien zur

Manipulation antizipierter Interdependenzverhältnisse auf offensive oder defensive Cyberproxys zugreifen können, wenn sie es wollen. Hierfür werden AkteurInnen auf vier Ebenen unterschieden: der staatlich-behördlichen, der privatwirtschaftlichen, der zivilgesellschaftlichen sowie der kriminellen Ebene.

3.4.1 Autokratien

Die zur Verfügung stehende Auswahl der Mittel im offensiven Cyberbereich wird entscheidend durch die jeweiligen Entwicklungen eines Landes im Sektor der Information and Communication Technology (ICT) beeinflusst. Diese wird definiert als die »*actual technology-based systems on which information is commonly stored and/or transmitted*« (Solms & van Niekerk 2013: 98). Während hierzu zu Beginn nur die Telekommunikation zählte, werden in diesem Konzept heute die immer stärker verschmelzenden Bereiche des Fernsehens, der Telefonie sowie des Internets, die zumeist durch einen einzigen ISP zu den EndnutzerInnen transportiert werden, zusammengefasst. Auf staatlich-behördlicher Ebene ist somit entscheidend, ob eine Autokratie bereits zu Beginn oder im Laufe des Untersuchungszeitraumes staatliche Einheiten in militärischen und/oder zivilen Behörden mit eigenen Fähigkeiten zur Durchführung offensiver Maßnahmen im Cyberspace etablierte. Ist dies der Fall und wurde dennoch eine offensive Cyberproxy-Nutzung bescheinigt, deutet dies aufgrund prinzipiell eigener technischer Fähigkeiten bereits auf eine geringere Erklärungskraft des staatlichen Motivs der technischen Ermächtigung durch Proxys hin. Möglich wäre jedoch eine anfängliche Unterstützung noch im Aufbau befindlicher Cybereinheiten durch Proxys, die schrittweise in diese integriert oder aber durch deren Handlungen obsolet werden könnten.

Auf privatwirtschaftlicher Ebene wird für die Bewertung der KV das Vorhandensein technologisch versierter IT-Unternehmen mit jeweilig autokratischer Herkunft analysiert. Wie bereits angedeutet wurde, können auch IT-Unternehmen für autokratische Regierungen offensive Cyberoperationen durchführen. Somit wird für die KV ein komprimiertes Lagebild privatwirtschaftlicher Technologieunternehmen mit mutmaßlich offensiven Cyberkapazitäten der jeweiligen Autokratie erstellt, um den prinzipiellen Proxy-Pool auf dieser Ebene bewerten zu können.

Auch der zivilgesellschaftliche Sektor kann Cyberproxys hervorbringen: Hierunter werden vor allem sog. HacktivistInnen, patriotische HackerInnen, aber auch Studierende/AbsolventInnen informationstechnologischer Studiengänge der autokratischen Fallbeispiele verstanden. Verfügt ein Land zu Beginn oder im Laufe des Untersuchungszeitraums über entsprechende AkteurInnen, so könnten diese bei Bedarf auch als Proxys eingesetzt werden.[14]

Zuletzt konstituiert der nationale Cyberkriminalitätssektor den dritten Proxy-Pool autokratischer Regime. So wird davon ausgegangen, dass Autokratien mit florierender Cyberkriminalität bei Bedarf auch entsprechend auf diese zurückgreifen werden, um Cyberoperationen zu ermöglichen. Entscheidend wird hierbei jedoch im Rahmen der

14 So könnten in heimischen Universitäten, oder aber im Ausland ausgebildete Informatikstudierende, als AgentInnen rekrutiert, oder aber in weniger institutionalisierten ad hoc-Beziehungen temporär als Proxys genutzt werden (Bronk und Tikk-Ringas 2013, S. 8).

Analyse der AV II sein, wie sich das Staat-Proxy-Verhältnis im jeweiligen Fall charakterisieren lässt, ob durch finanzielle Anreize, patriotische Gesinnung oder aber physischen/rechtlichen Zwang. Theoretisch formuliert beeinflusst die KV somit auf autokratischer Seite, ob die aufgrund konfliktiver Präferenzinkompatibilitäten wahrgenommenen Verwundbarkeitsasymmetrien mithilfe offensiver Cyberproxys überhaupt zum eigenen Vorteil gestaltet werden *könnten*. Die Cyberproxy-Nutzung durch Autokratien mit ausreichenden staatlichen Fähigkeiten und Ressourcen im ICT-Bereich betont zudem die beschriebenen politischen Funktionen der nichtstaatlichen StellvertreterInnen auf republikanischer Ebene nach innen und außen.

Hinsichtlich der (zumindest zu Beginn des Untersuchungszeitraums) vorliegenden Dominanz militärischer oder ziviler AkteurInnen im offensiven Cyberbereich könnte hierbei zudem von Belang sein, welche der beiden Seiten in der historischen Entwicklung der staatlichen ICT-Kapazitäten bzw. bei der Etablierung staatlicher Cyberfähigkeiten die Oberhand hatte. Dies könnte erklären, welche AkteurInnen den anfänglichen Cyberkonfliktaustrag und somit auch die Proxy-Nutzung aufgrund ihres auch im Cyberspace stärker ausgeprägten Herrschaftszugangs zum jeweiligen Zeitpunkt hauptsächlich bestimmten.

3.4.2 Demokratien

Um die primär defensive Cyberproxy-Nutzung demokratischer Staaten erklären zu können, kommt der KV ein noch größerer Stellenwert zu als im Falle der Autokratien. Analog sagt sie jedoch nicht notwendigerweise etwas darüber aus, ob eine Demokratie tatsächlich auf defensive Cyberproxys zurückgreift. Auf Seiten der Demokratien entscheidet sich jedoch bereits bei der jeweiligen Ausprägung der KV, ob nationale IT-Firmen stellvertretende Attribution überhaupt durchführen könnten und ob deren Berichte auch die notwendige Aufmerksamkeit erfahren würden.[15] Wie bei der Konzeptualisierung der AV aufgezeigt, wird im Falle demokratischer Proxys von einer primären Fokussierung auf nationale AkteurInnen ausgegangen, da für ausländische Proxys der für Demokratien von vornherein als schwächer anzunehmende Delegationsmechanismus im Falle defizitärer Ressourcen kaum mehr glaubwürdig plausibilisiert werden kann. Somit gilt es auch im Falle demokratischer Cyberproxy-Nutzung im Rahmen der empirischen Analyse zu untersuchen, inwiefern die privatwirtschaftlichen Potenziale im Cyber-Threat-Research-Bereich des Landes einen Einfluss hierauf hatten. Verfügt eine Demokratie in nicht ausreichendem Maße über technisch sophistizierte, mit hinreichender internationaler Reputation und Reichweite ausgestattete IT-Firmen, sind ihre Möglichkeiten zur defensiven Cyberproxy-Nutzung von vornherein eingeschränkt, auch wenn die Ausprägung der UV für einen solchen Gebrauch spricht.

---

15 Im Rahmen der »*weaponization of interdependencies*« von Farrell and Newman 2019 würde dies deren sog. »*panopticon*«-Effekt entsprechen: Bei diesem können Staaten zur »*weaponization*« ihrer privilegierten Stellung in globalen Netzwerken die hierbei an den Knotenpunkten gesammelten Informationen gezielt zum eigenen Vorteil verwenden, so wie auch Demokratien mit entsprechenden ICT-Niveaus die Daten/Erfahrungen ihrer nationalen IT-Firmen mit Zugang zu globalen Kundendaten zur Manipulation asymmetrischer Interdependenzbeziehungen einsetzen können.

3.5 Der Einfluss konventioneller Konfliktdynamiken als intervenierende Variable

Als intervenierende Variable (IV) fungiert das allgemeine Konfliktniveau bzw. dessen Dynamiken im Hinblick auf dessen Eingreifen in die Beziehung zwischen UV und AVs. Wie bei der Konzeptualisierung von AVs und UVs teilweise bereits angedeutet wurde, können Konfliktgeschehnisse der analogen Welt sowohl auf autokratische als auch demokratische Cyberproxy-Strategien erheblichen Einfluss nehmen.

3.5.1 Autokratien

Der Nutzen offensiver Cyberoperationen, entweder zur Vermeidung gewaltsamer konventioneller Konflikte oder zur erfolgreichen Gestaltung derselbigen, wurde in der Forschung unterschiedlich beurteilt. Besonders in Folge von Stuxnet wurde dem Internet eine geradezu potenziell pazifizierende Wirkung attestiert: Speziell Sabotage und Spionage wurden dabei im Rahmen eines »*Cool War*« im Cyberspace als mögliche Game-Changer im staatlichen Konfliktaustrag benannt (Arquilla 2012; Rid 2013). Entgegen der ebenfalls weit verbreiteten Eskalationsbefürchtungen ermögliche die diskutierte Offense-Dominance im Cyberspace somit gerade eine friedlichere, analoge Sphäre und unter der Bedingung der bis dato noch nicht erfolgten menschlichen Verluste in Folge eines Cyberangriffs. Im Sinne des »*ex-ante bargaining*« nach Fearon (1995, S. 380) seien Cybertools eine Option, um drohende offene und gewaltsame Konflikte doch noch abwenden zu können (Brantly 2014, S. 465). Durch sie können laut Brantly die Aspekte der »*information asymmetries, issue indivisibilities, and commitment problem*« und somit auch die Wahrscheinlichkeit eines offenen Krieges vermindert werden (2014, S. 472).[16]

In Folge der immer deutlicher werdenden Zurückhaltung von Staaten gegenüber Stuxnet ähnelnden regelmäßigen Cyberoperationen wurde dieses zielgerichtete ›Coercion‹-Potenzial von Cyberangriffen jedoch immer stärker angezweifelt. Stattdessen seien Cybertools überwiegend als Komplementärstrategien im Rahmen traditioneller Konfliktaustragungspfade zu verstehen, da sie nur in Kombination mit diesen eine ›coercive‹ Wirkung entfalten würden (Borghard und Lonergan 2017; Valeriano et al. 2018, S. 3). Cyberoperationen wird somit immer stärker das Potenzial zur Herbeiführung einer Verhaltensänderung bei einem gegnerischen Akteur abgesprochen, insbesondere bei einem bereits in Gang gesetzten konventionellen Konflikt (Kostyuk und Zhukov 2019). Aus diesem Grund wird in dieser Arbeit *nicht* argumentiert, dass der Einsatz von Cyberproxys auf militärischer Ebene eher zu Erfolgen oder Misserfolgen führen würde. Stattdessen soll durch die Konzeptualisierung der IV gezeigt werden, dass in Friedens- und Kriegszeiten unterschiedliche Anreize zu varianten Proxy-Nutzungen seitens unterschiedlicher autokratischer AkteurInnen wirken.

Für auf der konventionellen Ebene noch nicht militärisch eskalierte Konflikte sollten autokratische Cyberproxys eine stärkere Rolle zur Eskalationskontrolle zwischen der

16 Auch die Forschung zu Eskalationsdynamiken im Cyberspace deutet darauf hin, dass Cyberoperationen (zumindest in westlichen Demokratien wie den USA) eher als deeskalierendes Konfliktaustragungsmittel gesehen werden (Kreps und Schneider 2019).

konventionellen und Cyber-Konfliktebene spielen, insbesondere gegenüber konventionell militärisch überlegenen Demokratien. Befindet sich eine Autokratie jedoch bereits in einer militärischen Auseinandersetzung mit einem militärisch überlegenen Staat (potenziell begründet durch eine Allianzsituation), sollten Cyberproxys stärker der Manipulation der Verwundbarkeitsasymmetrie dienen, indem durch deren disruptiven Einsatz die größere Verwundbarkeit des Gegenübers im Cyberraum noch stärker ausgenutzt wird als in Friedenszeiten. Somit lautet die erste Hypothese hinsichtlich des Wirkens der IV:

> *H1: Je gewaltsamer das bestehende allgemeine Konfliktniveau ist, desto wahrscheinlicher ist auch ein intensiverer/disruptiverer Einsatz autokratischer Cyberproxys, etwa gegen kritische Infrastrukturen des Gegners.*

Aus Sicht der Plausible Deniability erscheint jedoch der Einsatz von Proxys bei bestehenden staatlichen Cyberfähigkeiten in einer solchen Situation weniger notwendig zu sein, da der Konflikt ja bereits gewaltsam eskaliert ist. Der offensive Einsatz autokratischer Cyberproxys in gewaltsamen konventionellen Konflikten könnte somit auf defizitäre staatliche Cyberkapazitäten hinweisen. Andererseits könnte dies darauf hindeuten, dass das Regime trotz eigener staatlicher Cyberfähigkeiten im Rahmen republikanischer Interdependenzbeziehungen gegenüber domestischen AkteurInnen wie dem Militär Proxys bevorzugt.

Hinzu kommt aus republikanischer Sicht, dass autokratische Regime bei der Entscheidung, ob sie einen Konflikt gewaltsam eskalieren lassen, weniger domestischen Restriktionen unterworfen sind als demokratische Regierungen. Wenn offensive Cyberangriffe zur Unterstützung militärischer Angriffe auf dem analogen Schlachtfeld dienen sollen, könnte es aus autokratischer Sicht sinnvoll erscheinen, beide Bereiche in ›eine Hand‹ und damit wahrscheinlicher in die des Militärs zu geben, da dieses in Kriegszeiten gegenüber zivilen Geheimdiensten meist einen verstärkten Herrschaftszugang innehat. Drei Aspekte tragen zu dieser erhöhten »*Organizational Salience*« des Militärs in Kriegszeiten bei (Legro 1996, S. 122):

1. Dessen Monopol über die Kriegsdomäne;
2. Die Komplexität der Kriegsdomäne, nochmals verstärkt durch das Hinzukommen des Cyberspace als ›Fifth Domain‹;
3. Der zeitlich begrenzte Entscheidungs- und Handlungskorridor.

Zudem ist der offensive Gebrauch von Cyberkonfliktmitteln im Sinne von Sabotage oder Disruption auch völkerrechtlich leichter in militärischer als in ziviler Verantwortung zu rechtfertigen (Boeke und Broeders 2018, S. 78). Somit lautet die zweite Hypothese im Hinblick auf das Wirken der IV:

> *H2: Je stärker die angewandten Cyberoperationen Verwundbarkeitsasymmetrien im Rahmen militärischer Konflikte manipulieren sollen, desto eher ist von einer militärischen Kontrolle autokratischer Cyberproxys auszugehen.*

Zusammenfassend kann somit konstatiert werden, dass für Autokratien, die sich bereits in gewaltsamen konventionellen Konflikten befinden, von einem intensiveren Ein-

satz der stärker militärisch geführten Cyberproxys auszugehen ist. Gleiches gilt für sich intensivierende, bislang gewaltfreie Konflikte, jedoch ohne die notwendigerweise verstärkte militärische Proxy-Anleitung. Dagegen ist in friedlicheren Zeiten nicht nur die Verschleierung der eigenen Urheberschaft, sondern auch der Tat an sich öfter das Ziel.

3.5.2 Demokratien

Auch für die Proxy-Nutzung demokratischer Staaten wird deren allgemeine Konfliktinvolvierung als IV konzeptualisiert. Grundlegend bedingen die aufgezeigten Inkompatibilitäten zu den Präferenzordnungen vor allem autokratischer Staaten mit größerer Wahrscheinlichkeit eine stärkere demokratische Involvierung in gewaltsame konventionelle Konflikte. Demokratische Regierungen führen aus unterschiedlichen Motivlagen mit überwiegend autokratischen Kontrahenten Krieg. Politische, militärische und ideelle Beweggründe bilden die hierbei mögliche Spannbreite ab.[17] Steht die autokratische Interessensdurchsetzung auf außenpolitischer Ebene den Interessen demokratischer Regierungen gleich auf allen drei Ebenen im Weg, müsste dies dem liberalen Argument nach wahrscheinlicher zu konventionellen Konflikten zwischen den Parteien führen. Damit wird nicht behauptet, dass Krieg in jedem Falle das unumgängliche Resultat einer solchen Konstellation sei, lediglich wird eine größere Wahrscheinlichkeit dieses Outcomes plausibilisiert.

Für die Attribution als defensive Cyberproxy-Tätigkeit bedeutet dies, dass die Involvierung demokratischer Staaten in konventionelle Konflikte deren Attraktivität für Cyberangriffe aus autokratischer Sicht verstärken kann. Obgleich auch in Friedenszeiten von Cyberoperationen autokratischer KontrahentInnen ausgegangen wird, könnten deren Häufigkeit und Intensität im Kontext gewaltsamer Auseinandersetzungen zunehmen (komplementär zur H1 der IV bei Autokratien). Als Konsequenz könnte der Handlungsdruck auf die Regierung in Folge von Cyberangriffen auf kritische Infrastrukturen oder zivile Ziele steigen.[18] Somit lautet für demokratische Staaten die erste Hypothese zum Wirken der IV:

> *H1: Je stärker die asymmetrische Verwundbarkeit demokratischer Staaten im Cyberraum im Rahmen gewaltsamer konventioneller Konflikte seitens Autokratien manipuliert/ausgenutzt wird, desto wahrscheinlicher ist eine demokratische Cyberproxy-Nutzung.*

Eine alternative Schlussfolgerung wäre jedoch, dass demokratische Regierungen, die sich bereits in einem gewaltsamen konventionellen Konflikt mit einer oder mehreren Autokratien befinden, auch weniger davor zurückschrecken sollten, selbst Cyberangriffe zu attribuieren, da die allgemeine Eskalation des Konfliktes ja bereits erfolgt ist. Sollte dies regelmäßig der Fall sein, so wäre jedoch nach wie vor die Frage, welche Formen

17 Wenn die eigenen ideellen Werte anscheinend (oder auch nur scheinbar) in Gefahr sind und das Wahlvolk aufgrund historischer Pfadabhängigkeit ein positiveres Verhältnis zum eigenen Interventionismus hat, kann dieses Vorgehen bei ausreichender Erfolgsaussicht sogar seitens der BürgerInnen mitgetragen werden (Lacquement 2004, S. 43).

18 Gleiches gilt für kommerzielle Ziele im Falle der beschriebenen Handelskonflikte mit einem entsprechend hohen Intensitätsniveau.

die jeweilige Verantwortungszuweisung politischer EntscheidungsträgerInnen dabei annimmt und welchen Einfluss der demokratische Subtypus hat, gerade im Hinblick auf damit verbundene politische Reaktionen.[19] Diese Überlegungen werden in folgende Hypothese überführt:

> *H2: Je stärker eine demokratische Regierung bereits auf der konventionellen Ebene Sanktionsmöglichkeiten gegenüber einem autokratischen Cyberangreifer in Stellung gebracht oder angewandt hat, desto wahrscheinlicher ist eine lediglich substituierende Proxy-Attribution.*

3.6 Staaten und ihre Proxys: Die Suche nach dem perfekten Match

Der vorgestellte liberale Erklärungsansatz regimetypenspezifischer Cyberproxy-Strategien beruht in erster Linie auf der komplexen Wirkweise unterschiedlicher domestischer Präferenzkonstellationen mit varianten Verwundbarkeitsasymmetrien auf den drei Liberalismus-Ebenen als Folge. Diese asymmetrischen Vulnerabilitäten zum eigenen Vorteil zu manipulieren, wird dabei als der übergeordnete Zweck autokratischer und demokratischer Cyberproxy-Aktivitäten angesehen. Das grundlegend inverse Verhältnis zwischen der eigenen Verwundbarkeit nach innen und außen begründet dabei die für Autokratien offensive Nutzung vs. der defensiveren Instrumentalisierung seitens demokratischer Regierungen. Aufgrund der unterschiedlichen Verwundbarkeiten auf der konventionellen und Cyber-Ebene nutzen Autokratien regelmäßiger letztere, um ihre Unterlegenheit im analogen Bereich auszugleichen. Dabei visieren sie insbesondere demokratische Informationsasymmetrien auf republikanischer Ebene an, was wiederum den Bedarf an demokratischer Proxy-Nutzung zur Folge hat, um diese Verwundbarkeitsasymmetrie zum eigenen Vorteil zu manipulieren.

Kein Gegenstand der vorliegenden Arbeit, jedoch für die Zukunft von Interesse könnte sein, inwiefern Demokratien versuchen sollten, auf analogem Wege die zugunsten autokratischer Regime ausgestalteten Informationsasymmetrien gegenüber deren Bevölkerungen aufzuweichen, ohne ihnen Vorwände für weitere Repressionsmaßnahmen zu liefern.

Grundlegend wird für beide Regimetypen die jeweilige Cyberproxy-Strategie als prävalent angesehen. Dennoch zeigt die Konzeptualisierung der KV und IV, dass davon unabhängig länder- sowie kontextspezifische Faktoren ebenfalls einen Einfluss auf den Zusammenhang zwischen UV und AVs nehmen können, sodass eben nicht davon auszugehen ist, dass alle Autokratien und alle Demokratien Cyberproxys gleichermaßen nutzen. Inwiefern jedoch zumindest für die vier Untersuchungsfälle deren Cyberproxys das ›perfekte Match‹ für das jeweils angestrebte Eskalationsmanagement darstellen, muss die empirische Analyse zeigen. Zuvor werden jedoch das Untersuchungsdesign sowie die dabei angewandte Methodik vorgestellt.

---

19 Falls die Demokratie jedoch trotz bereits erfolgter Kampfhandlungen weitere Eskalationen auf der konventionellen Ebene verhindern wollen sollte, könnte dies dennoch für die vermutete Cyberproxy-Nutzung sprechen. In ihrer 2021 veröffentlichten Dissertation beschäftigte sich bereits Heajune Lee mit dem Einfluss der Eskalationsrichtung einer Konfliktdyade auf das öffentliche Cyberattributionsverhalten der USA.