4. Das Mixed-Methods-Forschungsdesign

Das vorliegende Forschungsdesign folgt einem zweistufigen Aufbau. Der HD-CY.CON-Cyberkonfliktdatensatz bildet die Grundlage für den ersten quantitativen Analyseschritt. Hierbei werden die Daten im Sinne der deskriptiven Statistik aufbereitet und ausgewertet. Die daraus entstehenden Grafiken und Schaubilder eröffnen den Blick auf die vorherrschende staatliche Proxy-Nutzung und legen somit die Grundlage für die anschließende Fallauswahl. In einem zweiten Schritt erfolgt die eigentliche Analyse im Rahmen des strukturiert-fokussierten Vergleichs, um durch die qualitative Untersuchung der quantitativ ausgewählten Fälle die notwendige Analysetiefe zu erhalten. Das Untersuchungsdesign gehört somit zur Kategorie der Mixed Methods (Kelle 2014, S. 153).

Im Folgenden wird die empirische Datenbasis der Arbeit genauer vorgestellt: Der HD-CY.CON ist ein Cyberkonfliktdatensatz, der seit 2016 an der Universität Heidelberg im Rahmen mehrerer Forschungsprojekte entstanden ist und fortgeführt werden soll.[1] Die Autorin war seit 2017 an der Konzeptualisierung und Kodiertätigkeit des Datensatzes beteiligt (ab 2019 hauptverantwortlich), weshalb ein entsprechender Zugang sowie die notwendigen Kenntnisse im Umgang mit dem Datensatz bestehen.

Zunächst werden jedoch Erschwernisse sowie bestehende Forschungsprojekte im adressierten Forschungsfeld identifiziert und diskutiert.

4.1 Methodische Herausforderungen im Bereich der Cyberkonfliktforschung

»*Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake*« (Valeriano und Maness 2018, S. 50). Zu dieser Einschätzung gelangten Brandon Valeriano und Ryan C. Maness nicht etwa zu Beginn des sog. ›Cyber-Hypes‹, der sich in Folge des

1 Von 2016–2017 und 2017–2018 im Rahmen zweier Förderlinien der Exzellenzinitiative der Universität Heidelberg (Field of Focus-4), sowie grundlegend von 2019–2021 seitens der Deutschen Stiftung Friedensforschung innerhalb des Projektes »Sicherheit durch Verschleierung: Warum Regierungen Proxies in Cyberkonflikten einsetzen«.

ersten ›Cyber-Wars‹ in Estland 2007, der Cyberangriffe auf Georgien 2008 sowie des Bekanntwerdens von Stuxnet 2010 entwickelte, sondern im Jahr 2018. Das Attributionsproblem, ungleich verteilte Ressourcen zu dessen Lösung sowie Geheimhaltungserwägungen im Zusammenhang mit Cyberoperationen auf Angreifer- und Opfer-Seite wurden dabei bislang seitens der Forschung als zentrale Widrigkeiten hinsichtlich quantitativer Vorhaben im Bereich der Cyberkonfliktforschung angeführt (Hansel und Nanni 2018, S. 215; Griffith 2018; Healey 2018). In ihrer Arbeit aus 2018 befassten sich Valeriano und Maness mit den Grenzen und Möglichkeiten der Quantifizierung von Cyberkonflikten. Darin plädieren sie dafür, dass trotz der unstrittigen Herausforderungen in *jedem* Forschungsfeld einmal ein Anfang gemacht werden muss(te). Somit sollten quantitative Cyberkonfliktprojekte vermehrt angegangen, dabei jedoch stets hinsichtlich potenzieller Verzerrungen oder theoretischer Einschränkungen reflektiert werden. Dies sei eine Grundherausforderung, besonders auch für informierte Entscheidungen politischer EntscheidungsträgerInnen, die sich mit Cyberkonflikten konfrontiert sehen.

An den Grundsatz »*Reality is a Social Construction*« (Valeriano und Maness 2018, S. 51) knüpft auch der HD-CY.CON an, der nicht etwa den Anspruch postuliert, sämtliche vorgefallene Cyberoperationen zwischen staatlichen und/oder nichtstaatlichen AkteurInnen erfassen zu können, sondern durch die Beleuchtung der öffentlich sichtbaren Angriffe sowie des politischen Umgangs damit wichtige Dynamiken des Forschungsgegenstandes offenzulegen.[2]

Valeriano und Maness arbeiteten zum Zeitpunkt des oben genannten Zitates bereits an der zweiten Version ihres ›Dyadic Cyber Incident and Dispute Datasets‹ (DCID), dessen erste Fassung rein staatliche Cyberattacken zwischen bereits bekannten Rivalen für die Jahre 2001 bis 2011 umfasste (insgesamt 110 Vorfälle; Valeriano und Maness 2014, S. 356). Der DCID stellte in einer bis dato auf qualitative Fallstudien konzentrierten Forschungslandschaft den ersten Versuch dar, die nur schwer zugängliche Cyberkonfliktlandschaft auch quantitativ zu vermessen. Somit konnten die Autoren in der Folge zwei ihrer zentralen theoretischen Thesen durch ihre empirischen Daten stützen: Zum einen die bereits beschriebene These der staatlichen Zurückhaltung (restraint) im Cyberspace, die das relativ niedrige Konfliktniveau im Cyberspace trotz weitreichender technischer Möglichkeiten aus verschiedenen Perspektiven zu erklären vermag (Valeriano und Maness 2014; Valeriano und Maness 2015; Borghard und Lonergan 2019). Zum anderen indizierten ihre gesammelten Cyberkonfliktdaten eine fast nicht nachweisbare Beziehung zwischen der konventionellen und Cyber-Konfliktebene im Sinne eines potenziellen Spill-Overs (Maness und Valeriano 2016a), was in der Folge von weiteren Autoren bestätigt wurde (Kostyuk und Zhukov 2019).

Somit wurde erstmals eine Alternative zum bis dato vorherrschenden methodischen Vorgehen offeriert, das über den Vergleich weniger Cyberoperationen (desselben Cyberangreifers) zumeist nicht hinausreichte (u.a. Hjortdal 2011; Axelrod und Iliev 2014; Blank

2 Die Metapher eines Eisberges, bei dem stets nur der Teil oberhalb des Wasserspiegels sichtbar ist, wird für das Deepweb verwendet (Bergman 2001) und greift auch für Cyberoperationen: Auch wenn ein signifikanter Teil von Attacken stets im Verborgenen bleiben wird, so können über die umfassende Analyse des sichtbaren Teils dennoch wichtige Erkenntnisse über deren Wirkweise und Auswirkungen gewonnen werden.

2017; Ji-Young et al. 2019). Nichtsdestotrotz konnte bislang auch der DCID aufgrund seines inhaltlichen Zuschnitts auf rein staatliche Konflikttätigkeit, zudem zwischen bereits in der analogen Welt rivalisierten Staaten, sowie weiterer Einschränkungen für viele theoretische Fragen keine adäquate empirische Grundlage bilden. Zu nennen wäre die wenig bis kaum ausdifferenzierte Kodierung der Kategorie des attribuierten Angreifers, wobei nicht zwischen direktstaatlichen sowie staatlich gelenkten/unterstützten Proxy-Angriffen unterschieden wird.[3]

Des Weiteren erlaubt der DCID keine Aussagen über die jeweilige Quelle der Attribution, d.h., wer die Verantwortungszuweisung im jeweiligen Fall vorgenommen hat. Auch werden nicht nur Cyberoperationen mit tatsächlich öffentlich bekannter Verletzung der CIA-Triade vom DCID inkludiert, sondern auch lediglich ›versuchte‹ Cyberoperationen.[4] Kritisch zu betrachten ist auch die in Version 1.5 eingeführte ›Interaction-Type‹-Kategorie: Hierbei erfolgt implizit eine Interpretation der Motivlage des Cyberangreifers, nämlich hinsichtlich der Frage, ob es sich um eine Defensiv- oder Offensivoperation gehandelt hat (Maness et al. 2019, S. 5). Den Anfang einer Cyberkonfliktinteraktion auszumachen, ist aufgrund potenziell nicht öffentlich gemachter Angriffe schwierig, weshalb auch eine Klassifizierung einer scheinbar lediglich auf Verteidigung ausgerichteten Cyberoperation zumindest hinterfragt werden muss.[5] Des Weiteren erschwert der bereits herausgestellte Unterschied zwischen lediglich auf allgemeine Spionage ausgerichteten Infiltrationen fremder Netzwerke und der als Vorstufe einer potenziell folgenden Manipulation des Zielsystems dienenden Infiltration eine solche Bewertung.

Einen weiteren Forschungsansatz im Bereich der stärker quantitativ basierten Cyberkonfliktforschung stellt die ›Cyber-Event-Liste‹ des Center for Strategic and International Studies (CSIS) dar, eine rein beschreibende Auflistung von Cyberoperationen ohne systematische Kriterien der Attribution, der Angriffs-Kategorisierung oder der Intensität (CSIS 2020). Im Gegensatz hierzu fokussiert sich der ›Cyber Operations Tracker‹ des Council on Foreign Relations (CFR) auf »*state-sponsored cyberattacks*« (CFR 2020). Somit ignoriert dieser jedoch Cyberoperationen vonseiten nichtstaatlicher AkteurInnen, die

3 Im Rahmen der Veröffentlichung der Version 1.5 des DCID, im Juni 2019, kündigten die Autoren an, in der künftigen Version 2.0 erstmals auch nichtstaatliche AkteurInnen sowie alle möglichen Staaten-Dyaden erfassen zu wollen. Version 1.5 legte einen größeren Fokus auf den jeweiligen Kontext der Cyberoperationen und führte neue Variablen ein, wie die Kategorie der »*cyber-enabled information-operations*« (Maness et al. 2019, S. 2). Zum Zeitpunkt der Einreichung dieser Arbeit stand Version 2.0 jedoch noch nicht der Öffentlichkeit zur Verfügung.

4 So wird der Zweck einer Kategorie der Version 1.5 wie folgt beschrieben: »*Whether or not the incident successfully achieved its objective; did it breach the target's network and fulfill its intended purpose*« (Maness et al. 2019, S. 4). Für eine derartige Bewertung bedarf es jedoch einer plausiblen Einschätzung dieses »*objective*« des jeweiligen Angreifers, was aufgrund des beschriebenen Cybersicherheitsdilemmas oft erschwert wird.

5 Die Unterscheidung, ob eine Operation defensiver oder offensiver Natur ist, hängt zudem von dem Wissen über potenziell zuvor erfolgte Operationen innerhalb der betreffenden Konfliktdyade ab. Darüber hinaus können sprachliche Darstellungen der Operationen erheblichen Einfluss auf eine solche Interpretation nehmen und sich nicht mit der Interpretation des jeweiligen Opfers decken, der die Operation womöglich nicht als defensiv empfunden hat. Bemerkenswert ist zudem, dass einer der beiden Urheber des DCID, Brandon Valeriano, ansonsten gegen die Anwendung der ›Offense vs. Defense‹-Unterscheidung im Cyberspace plädiert (Valeriano 2021).

ebenfalls politische Wirkung entfalten können. Die Beurteilung, dass der jeweilige Fall als staatlich gesponsert zu bewerten ist, geht zudem nicht in jedem der erfassten Angriffe aus den verlinkten Quellen hervor (z.B. für die Gruppierung ›Hellsing‹), was jedoch in einzelnen Fällen auch auf den DCID zutrifft, z.B. für dessen Südkorea-Attribution des sog. ›Earthquake-Hacks‹ aus 2011. Zudem wird (ebenfalls bei beiden Projekten) über eine mögliche Anfechtung der Attribution durch andere AkteurInnen keine Auskunft gegeben. Ebenso fehlt (beim CFR-Tracker) eine Kategorie zur Bewertung der jeweiligen Intensität bzw. Schwere des Vorfalls.

Gemein ist allen drei genannten Ansätzen (DCID; CSIS; CFR), dass sich diese ausschließlich auf englischsprachige Quellen beziehen. Somit könnte eine potenzielle Verzerrung im Sinne regionaler bzw. sprachlich-kultureller Blindflecken bei der Aufnahme relevanter Cyberoperationen die Folge sein (Sparks 2003). Zudem würde die Inklusion nicht englischsprachiger Quellen die Möglichkeit bieten, potenziell existierende konkurrierende Attributionen zu bestimmten Fällen zu ermitteln und somit politisch motivierte Verantwortungszuweisungen als solche zu entlarven (Zetter 2017b).

4.2 Der HD-CY.CON-Datensatz

Aufbauend auf der Konfliktdefinition des Heidelberger Instituts für Internationale Konfliktforschung (HIIK) werden Cyberkonflikte im Rahmen des HD-CY.CON als eine »*Interesseninkompatibilität zwischen mindestens zwei AkteurInnen im Hinblick auf einen bestimmten Konfliktgegenstand*« (HIIK 2016, S. 6), ausgetragen durch Cyberoperationen, definiert. Orientiert am Kernverständnis von IT-Sicherheit, werden in der Arbeit hierunter Handlungen zusammengefasst, die einen oder mehrere Bereiche der sog. CIA-Triade der Informationssicherheit verletzen (Confidentiality; Integrity; Availability; Andress 2014, S. 5). Diese interaktionistische Konfliktdefinition und das differenzierte Kodierverfahren (siehe Abschnitt 4.2.1) ermöglichen eine detailliertere Betrachtung der politischen Dimension des Konfliktaustrags, etwa der Salienz erfasster Cyberkonfliktgegenstände (Steiger et al. 2018, S. 84). Demokratien werden entsprechend des ›Freedom in the World Index‹ von Freedom House anhand des Labels »*free*« im entsprechenden Operationsstartjahr definiert, gleiches gilt für autokratische Staaten hinsichtlich der Kategorisierung »*not free*« (Freedom House 2019).

4.2.1 Theoretische Annahmen und Implikationen

Zunächst gilt es zu klären, welche Arten von Cyberoperationen für den HD-CY.CON relevant sind und auf Grundlage welcher Kriterien deren Bewertung erfolgt. Wie Valeriano und Maness richtig konstatieren, bedeutet die Festlegung dieser Inklusionskriterien einen entscheidenden Schritt im Prozess der Entwicklung jedes Konfliktdatensatzes (Valeriano und Maness 2018, S. 57). Der HD-CY.CON wendet hierbei drei grundlegende Kriterien an (Harnisch et al. 2021, S. 1):

1. Deutet die Attribution auf einen staatlichen Angreifer, einen staatlich unterstützten Angreifer (Proxy) oder einen nichtstaatlichen Akteur mit offensichtlich politischer Motivation (z.B. das Hackerkollektiv Anonymous) hin?[6]
2. Ist ein politisches Ziel oder sind mehrere politische Ziele unter den Opfern, z.B. Politiker, Ministerien, staatliche Verwaltungsbehörden oder militärische bzw. polizeiliche Einrichtungen?[7]
3. Wurde die Cyberoperation im Sinne einer verbalen Adressierung des Vorfalles durch PolitikerInnen politisiert?[8]

Trifft eines (oder treffen mehrere) dieser Inklusionskriterien zu, wird der recherchierte Angriff in den Datensatz aufgenommen und anhand des Codebooks kodiert. Wichtig ist zudem, dass informationsbasierte Beeinflussungsoperationen wie Fake News, die nicht die CIA-Triade der Informationssicherheit verletzen, entsprechend dem technisch dominierten Verständnis von Cybersicherheit kein Gegenstand des Datensatzes sind (Schünemann 2020, S. 202). Des Weiteren muss ein erkennbarer Schaden aus den erfassten Quellen hervorgehen, lediglich versuchte Operationen fallen somit ebenfalls aus dem Datensatz heraus (Steiger et al. 2018, S. 90).

Die drei Inklusionskriterien veranschaulichen die möglichst große Spannbreite an Cyberoperationen mit potenziell politischer Dimension, die seitens des HD-CY.CON abgedeckt werden. Dabei erfüllt er zudem Forderungen aus der Forschung an künftige Vorhaben, z.B. die differenzierte Inklusion nichtstaatlicher AkteurInnen sowie von Cyberoperationen im Rahmen innerstaatlicher Repression (Valeriano und Maness 2018, S. 57).

Im Folgenden werden zentrale theoretische Aspekte des HD-CY.CON und seines zugrunde liegenden Codebooks vorgestellt und diskutiert.

4.2.1.1 Attribution

Die Bedeutung der Attribution von Cyberoperationen reicht immer stärker über die rein technische Ebene hinaus und wird zunehmend zum Politikum. Der HD-CY.CON trägt diesem Umstand in besonderer Weise Rechnung: Durch eine multiperspektivische Kodierung von Attributionen wird die Offenlegung unterschiedlicher Attributionslogiken möglich. Auch wenn an dieser Stelle die bereits dargelegte technische Komplexität der Attribution von Cyberangriffen keinesfalls als trivial abgetan werden soll (vgl. Rid und Buchanan 2015; Berghel 2017), lassen sich durch dieses Vorgehen dennoch die unterschiedlichen Attributionsmaßstäbe der verschiedenen AkteurInnen erfassen. Für jeden im Datensatz kodierten Fall wurden möglichst sämtliche potenziell getätigten Verantwortungszuweisungen recherchiert: des Opfers selbst, der Regierung des jeweiligen Opfers (falls es sich dabei z.B. um eine Firma gehandelt hat), des Täters,[9] der IT-Sicherheits-

6 AkteurInnen wie Anonymous oder andere, nichtstaatliche CyberangreiferInnen mit politischer Motivation werden als ›Hacktivists‹ bezeichnet.

7 Eine detaillierte Auflistung der politischen Ziel-Kategorien findet sich im frei zugänglichen Codebook des HD-CY.CON.

8 Bestreitet ein beschuldigter Staat lediglich die Schuld an einer Cyberoperation, so wird dieser Sprechakt im Rahmen des HD-CY.CON noch nicht als Politisierung bewertet.

9 Eine solche Selbstzuschreibung ist jedoch bislang überwiegend bei HacktivistInnen wie Anonymous vorzufinden, oder auch nichtstaatlichen, patriotischen Hackergruppierungen, deren zu-

branche sowie anderer DrittakteurInnen wie Forschungsinstituten oder Geheimdiensten befreundeter Staaten (Steiger et al. 2018: 84).[10] Jede Attribution wird dabei in zwei Kategorien unterteilt: das attribuierte Land des oder der Täter(s) sowie die Kategorisierung des Akteurs/der AkteurInnen.[11] Dabei muss nicht für beide Kategorien in jedem Fall eine Attribution vorliegen. So werden Cyberoperationen oftmals lediglich einem geografischen Ursprung zugeordnet, ohne jedoch weitere Aussagen über die genauen TäterInnen zu treffen, und umgekehrt. Wichtig ist hierbei, dass, anders als beim Cyber Operations Tracker des CFR, eine gewisse Eindeutigkeit bei der Attribution gewährleistet sein muss.[12] Äußert etwa eine IT-Firma, dass eine seriöse Attributionsbewertung nicht möglich ist, auch wenn einige Spuren in eine Richtung deuten, so wird die Initiator-Category (=Angreifer-Kategorie) seitens der IT-Sicherheitsbranche für diesen Fall mit ›0‹ und damit als ›unknown‹ kodiert.

Die Inklusion der Attributionen des Privatsektors in Form eigenständiger Cyber-Threat-Research-Berichte bzw. umfassender Analysen zu bestimmten Angriffen kann dabei helfen, rein politisch motivierte Attributionen als solche zu entlarven und im Sinne der technischen Evidenzen in Frage zu stellen (Steiger et al. 2018, S. 84). Unterstützt wird dieses Ansinnen durch die Kodierung der jeweiligen Länder, aus denen die attribuierenden IT-Firmen stammen, um potenzielle Verbindungen zu politischen Attributionstaktiken verschiedener Regierungen aufzeigen zu können.[13] Somit ist eine Vermessung des

---

meist ideologisch motiviertes Ziel es ist, dass das anvisierte Opfer (und bestenfalls die ganze Welt) von ihren Taten und Fähigkeiten erfährt. Eine Analyse zu dieser »*voluntary attribution*« erstellten (Poznansky and Perkoski 2018). Dabei identifizierten sie unterschiedliche Motivlagen für freiwillige Selbstattribution zwischen Staaten und nichtstaatlichen AkteurInnen. Erstere ließen sich hierauf vor allen Dingen dann ein, wenn der jeweilige Gegner im Sinne von coercion durch die Cyberoperation zu etwas gezwungen werden sollte, während nichtstaatliche HackerInnen hierdurch wie erwähnt in erster Linie ihre Fähigkeiten zur Schau stellen wollen (Poznansky und Perkoski 2018, S. 402). Auch Floyd untersuchte in einer Arbeit aus 2018, in welchen Fällen eine »*self-attribution*« und somit die Aufgabe des konstatierten »*attribution-advantage*« aus staatlicher Sicht Sinn ergibt. Jedoch lassen sich bislang eher selten freiwillige Verantwortungseingeständnisse von staatlicher Seite finden, ein Beispiel hierfür wären jedoch die selbst proklamierten (jedoch durch wenig operative Details unterfütterten) Cyberangriffe der USA sowie Großbritanniens auf Ziele des sog. Islamischen Staates (Seals 2018; Temple-Raston 2019).

10 Bekanntestes Beispiel für einen solchen Fall ist bis dato die Informationsweitergabe des niederländischen Geheimdienstes AIVD (Algemene Inlichtingen- en Veiligheidsdienst) an die US-Behörden im Vorfeld der Wahlmanipulation 2016. Der AIVD hatte Zugriff auf die Computer einer der involvierten russischen Hackergruppierungen, Cozy Bear und konnte somit deren Agieren gegen das DNC live mitverfolgen, die US-Behörden alarmieren sowie die im Nachgang erfolgte US-Attribution in Richtung des Kremls stützen, auch wenn dies vonseiten der Niederlande nicht öffentlich geschah (Noack 2018).

11 Auf staatlicher Seite sieht das Codebook folgende Initiator-Kategorien vor: ›State‹ (1), ›Non-state-actor‹, ›state-sponsorship suggested‹ (Proxy) (2) sowie ›Non-state-actor, state-sponsorship suggested, widely held view, but not invoked in this case‹ (2,1) (für Akteure, die im Allgemeinen als staatliche Proxies angesehen, im betreffenden Fall von der Attributionsquelle jedoch nicht konkret als solche benannt werden).

12 Wie bereits erwähnt, lassen sich manche Attributionseinordnungen des CFR Tracker anhand der angegebenen Quellen nicht nachvollziehen.

13 Die entsprechende Kategorie lautet ›Country of Origin: IT-Attribution‹ und befand sich noch nicht in dem von Steiger et al. 2018 vorgestellten Codebook.

vermuteten Graubereiches zwischen erfolgter technischer und nach wie vor oftmals unterlassener politischer Attribution möglich.

Die Gegenüberstellung politischer und stärker technisch basierter Attributionen der IT-Firmen ermöglicht zudem, potenzielle Widersprüchlichkeiten bestimmter Verantwortungs-zuweisungen aufzudecken (Steiger et al. 2018, S. 84). So kann es beispielsweise dazu kommen, dass Attributionen politischer AkteurInnen im Nachhinein nach erfolgten technischen Analysen seitens der IT-Sicherheitsbranche angezweifelt oder widerlegt werden. Der Grad der ›Contestation‹ von Cyberattributionen wird auch in der Forschung zunehmend untersucht (z.B. Egloff 2020a) und im HD-CY.CON auf Grundlage der Kategorie ›Attribution-Basis‹ wiedergegeben. Diese gibt an, von welchem Akteur die jeweils kodierte Attribution stammt. Bei potenziell mehreren attribuierenden AkteurInnen kann es hier auch zu mehrfachen Kodierungen kommen.[14] Finden sich widersprüchliche Attributionen verschiedener AkteurInnen, wird im Rahmen der Attribution-Basis-Kategorie zusätzlich zu den Codes der jeweiligen UrheberInnen der Verantwortungszuweisung der Code ›4‹ kodiert, der für eine ›Contested Attribution‹ steht. Die Beurteilung, welche Zuweisung plausibler ist, übersteigt jedoch den Anspruch des Datensatzes.

Da öffentliche Verantwortungszuweisungen oft erst nach einer gewissen Zeit erfolgen, kodiert der HD-CY.CON (wie auch der DCID) Cyberoperationen für einen bestimmten Zeitraum frühestens mit einem Jahr Abstand (Steiger et al. 2018, S. 81). Auch werden die getätigten Attributions-Kodierungen immer wieder notwendigerweise aktualisiert, da Attributionen im Cyberspace oftmals nicht als final angesehen werden können. Ein Beispiel wären False-Flag-Attacken (auch ›Fourth-Party-Collection‹ genannt; vgl. Guerrero-Saade und Raiu 2017), wie sie etwa im Falle der jahrelang seitens der russischen APT Turla gekaperten und für eigene Angriffe genutzten IT-Infrastruktur der iranischen APT OilRig 2019 bekannt wurden (Corera 2019).

4.2.1.2 Intensität

Die traditionelle Konfliktforschung sah lange Zeit die Mortalitätsrate eines Konfliktes als das entscheidende Kriterium dafür an, wie intensiv dieser zu bewerten sei und ob dabei bereits von einem Krieg gesprochen werden kann. Die prominentesten Beispiele hierfür sind der Correlates of War-Index (COW) sowie das Uppsala Conflict Data Program (UCDP). In der Folge kam es jedoch auch zu alternativen Ansätzen der Klassifizierung und Bewertung unterschiedlicher Konflikte: Das Konfliktbarometer des Heidelber-

14 Durch die zusätzliche Kodierung der Form der Attribution kann zudem ein regelmäßiges ›Durchstechen‹ von Attributionen mithilfe der Vierten Gewalt als mögliches Handlungsmuster vor allem in demokratischen Staaten aufgedeckt werden. Direkte, öffentlich getätigte Attributionen von staatlicher Seite wären dagegen: Erklärungen der Regierung, technische Berichte/Warnungen (alerts), öffentlich getätigte geheimdienstliche Bewertungen sowie strafrechtliche Anklageerhebungen oder Sanktionen (Romanosky und Boudreaux 2021). Hinzu kommt, dass auch Attributionen seitens zivilgesellschaftlicher Akteure, wie NGOs oder Forschungseinrichtungen erfasst werden (›Attribution by Third Party‹). Somit soll dem bereits identifizierten Bias zu Gunsten der Aufarbeitung von Cyberoperationen gegen kommerzielle AkteurInnen durch private IT-Firmen Rechnung getragen und hierdurch auch relevante Angriffe auf die Zivilgesellschaft umfassender abgebildet werden können (Maschmeyer et al. 2020).

ger Instituts für internationale Konfliktforschung bewertet Konflikte nicht nur anhand der Anzahl menschlicher Opfer, sondern auch durch die Betrachtung von verschiedenen Konfliktmaßnahmen, Konfliktereignissen und vor allem Konfliktgegenständen. Somit wird der Fokus nicht ausschließlich auf die gewaltsamste Form von Konflikten gelegt. Stattdessen wird im Rahmen eines Stufenmodells die Analyse potenzieller Transformationen in eskalativer oder deeskalativer Richtung ermöglicht (HIIK 2016).

Der DCID sieht im Gegensatz zu den eher deskriptiven CFR und CSIS eine eigene Intensitätsskala vor. Deren Zustandekommen bzw. die dieser zugrunde liegenden Bewertungskriterien konnten dabei jedoch nicht gänzlich transparent und konsistent sichtbar gemacht werden: So kann die beispielhafte Aufzählung einzelner Fälle zu den jeweiligen Kategorien keine alleinige und ausreichende Anleitung für Dritte liefern, die das Schema auf andere Fälle zu übertragen versuchen. Es bleibt somit unklar, wie konkret beispielsweise »*Type 4*«, also Incidents mit einem »*dramatic effect on a country*«, von »*Type 5*«, also Vorfällen mit einem »*escalated dramatic effect on a country*«, zu unterscheiden wären (Valeriano und Maness 2014, S. 353). Trotz dieser Defizite hinsichtlich der Übertragbarkeit der Intensitätsmessung liefert das Vorgehen des DCID wichtige und auch für den HD-CY.CON relevante Anhaltspunkte für das eigene Vorgehen: So sieht auch dieser die Möglichkeit vor, dass Cyberangriffe eine besonders schwerwiegende Auswirkung auf grundlegende Kernfunktionen einer betroffenen Gesellschaft haben können. Der sog. ›Target-Multiplier‹ beinhaltet eine Multiplikation des zuvor errechneten ungewichteten Intensitätswertes mit 1,5, für den Fall, dass der jeweilige Cyberangriff eine gesamtgesellschaftlich als besonders kritisch anzusehende Wirkung entfaltet hat. Dies trifft zu, wenn durch den Cyberangriff Teile der kritischen Infrastrukturen[15] so getroffen werden, dass daraus nicht nur partielle, sondern zumindest regionale Folgen erwachsen (beispielsweise flächendeckende Stromausfälle in einem Land oder die Beeinträchtigung der Wasserversorgung signifikanter Teile der Bevölkerung etc.), oder, wenn die nationalen Angriffs- oder Verteidigungskapazitäten und -fähigkeiten eines Landes durch den Angriff zumindest zwischenzeitlich erheblich gestört werden (bspw. durch das Paralysieren militärisch bedeutsamer Satelliten oder die Störung der Flugsysteme von Kampfjets etc.) (Steiger et al. 2018, S. 87). Im Wissen, dass diese Kriterien keinesfalls als ›hart‹ gelten und somit nicht durch konkrete Grenzwerte erfasst werden können, ergänzt dieser Multiplikator die eigentliche Intensitätsbemessung lediglich. Der ungewichtete Cyberintensitätswert entsteht vielmehr durch die Aufsummierung aller Werte in den verschiedenen technischen Kategorien des HD-CY.CON, die folgende Aspekte beinhalten: Art des Angriffes (Incident-Type) sowie potenzielle physische Schäden (räumlich und zeitlich). Aufgrund der nicht existierenden direkten Zuweisung menschlicher Todesopfer als Folge von Cyberangriffen (Lonsdale 2019) wird die ›Casualties‹-Kategorie bislang noch als eine ergän-

15 Die Definition der kritischen Infrastrukturen im Rahmen des HD-CY.CON erfolgte auf Grundlage der Selektion eines von möglichst vielen Staaten geteilten Verständnisses der hierunter zu fassenden Teilbereiche. Auch wenn z.B. die USA in Folge der Wahlen 2016 ihre Wahlsysteme ebenfalls als kritisch einstuften, traf dies bislang jedoch noch nicht auf das Gros der anderen Staaten zu. Falls sich dies in den kommenden Jahren ändern sollte, müsste die Kategorie entsprechend angepasst werden.

zende Zusatzkategorie geführt.[16] Physische Effekte werden erfasst, da untersucht werden soll, inwiefern die steigenden Potenziale für Cyberangriffe mit Auswirkungen ähnlich physischer Gewalt auch tatsächlich ausgenutzt werden. Gerade disruptive Angriffe auf kritische Infrastrukturen[17] werden am ehesten als gerechtfertigte Szenarien für den Begriff ›Cyberwar‹ genannt, was somit durch diese Kategorie gesondert erfasst werden kann (Nye 2011).

Der HD-CY.CON unterscheidet zwischen folgenden Angriffsarten: ›Data Theft‹ (mit oder ohne Doxing), ›Disruption‹, ›Hijacking‹ (mit oder ohne Missbrauch). Bei diesen Kategorien wird davon ausgegangen, dass sie am umfassendsten in der Lage sind, alle möglichen Varianten digitaler Angriffsstrukturen bzw. deren Auswirkungen abzubilden. Aufgrund der beschriebenen Schwierigkeit, Intentionen von CyberangreiferInnen zweifelsfrei festzustellen, ist die Erfassung der tatsächlichen Folgen unter Berücksichtigung von Kontextfaktoren, die zumindest partiell Aufschluss darüber geben können, ob es sich dabei um intendierte oder unintendierte Auswirkungen handelt, die gebotene Herangehensweise.[18] Unter Data Theft wird jede Form der vom Opfer unautorisierten Exfiltration von Daten des Zielsystems verstanden.[19] Das häufigste Einfallstor für CyberangreiferInnen stellen dabei nach wie vor technisch eher wenig sophistizierte Phishing-Kampagnen oder auch Social-Engineering-Methoden dar.[20] Jedoch kommen auch Watering-Hole-, oder Living-off-the-Land-Methoden häufig zum Einsatz (Bisson

16 In einer Studie von Choi et al. 2019 stellten die Autoren fest, dass in Krankenhäusern, die in Folgen von »*data breaches*« mit der Wiederherstellung der betroffenen Systeme zu kämpfen hatten, die Mortalitätsrate unter bestimmten Patienten in der direkten Folge anstieg, im Vergleich zum Zeitraum davor. Diese »*data breaches*« wurden in der Studie jedoch nicht ausschließlich durch Hacking-Angriffe wie Ransomware-Attacken herbeigeführt, sondern auch etwa durch finanziell motivierte Insiderhandlungen, wie das Leaken von Patientendaten (Choi et al. 2019, S. 974).

17 Die Groß- oder Kleinschreibung des Begriffsbestandteils ›kritisch‹ fand in der Fachliteratur bisher uneinheitlich statt. Im weiteren Verlauf wird daher die Kleinschreibung bevorzugt.

18 Orye und Maennel propagieren in ihrer Arbeit von 2019 eine »*Encompassing Taxonomy of Cyber Effects*«, die zwischen »*physical*«, »*digital*«, »*economic*«, »*psychological*«, »*political/reputational*« und »*social/societal*« Effekten von Cyberoperationen unterscheidet. Ein ähnlich umfassendes Vorgehen sieht zudem das »*Cyber Harm Model*« der Oxford University vor (Agrafiotis et al. 2016). Für eine Kodierung möglichst vieler Vorfälle, wie sie im Rahmen des HD-CY.CON praktiziert wird, wäre jedoch eine solche Kategorisierung von Cybereffekten aus forschungspragmatischen Gründen heraus nur schwierig bis kaum zu bewältigen. Nur für einen kleinen Teil der öffentlich bekannt gewordenen Angriffe existieren ausreichende Informationen für eine solch graduelle Kodierung, zudem wäre eine Bewertung der ursprünglichen Zielsetzungen der AngreiferInnen (im Gegensatz zu einer hauptsächlichen Erfassung der tatsächlichen Effekte) letzten Ende zumeist nur eine Interpretation.

19 Die nachfolgenden Ausführungen zur Veranschaulichung der Kodierpraxis in Bezug auf die Incident-Types und deren Intensitätsbewertungen basieren auf (Steiger et al. 2018, S. 86–89).

20 Phishing-Operationen stellen den Versuch dar, unrechtmäßigerweise an Daten/Informationen/Zugriffsrechte eines Ziels zu gelangen, indem man sich diesem gegenüber als vertrauenswürdige oder gar bekannte Person/Institution darstellt, z.B. via Phishing-Mails. Social-Engineering bezeichnet jede Form von Manipulation einer Person, die darauf abzielt, durch zumeist nicht-technische Betrugsformen an Daten/Informationen dieser Person zu gelangen. Dabei kann zuvor gesammeltes Wissen über diese Person ausgenutzt werden, oder aber generelles menschliches Fehlverhalten, etwa im Umgang mit E-Mail-Anhängen, aber auch die Hilfsbereit oder Angst einer Zielperson. Social Engineering ist jedoch nicht auf Online-Maßnahmen beschränkt (BSI 2021).

2018; Symantec 2018; UNODC 2019).[21] Zusätzlich können die abgegriffenen Daten in der Folge veröffentlicht (geleakt) werden, was ein Fall von Data Theft + Doxing wäre. Die Kategorie der Disruption beschreibt dagegen einen Cyberangriff, der die Störung einer Funktion oder mehrerer Funktionen des Zielsystems zur Folge hatte. Am häufigsten handelt es sich dabei um DDoS-Angriffe, die die Nichterreichbarkeit des Zielsystems durch Überlastung in Folge von massiv gehäuften Anfragen an den Zielserver bewirken. Ein weiteres Beispiel wäre der Missbrauch des Social-Media-Accounts eines Politikers. Hierbei bedarf es in der Regel keiner anspruchsvollen Hacking-Methoden, zumeist werden lediglich schwach gesetzte Passwörter ausgenutzt oder Phishing-Nachrichten im jeweiligen Netzwerk versendet. Somit wäre dies ein Fall der Disruption, jedoch ohne Hijacking, da hierbei die gestörte Funktionserfüllung des Social-Media-Accounts im Vordergrund stünde. Hijacking bezeichnet dagegen Fälle, in denen es AngreiferInnen gelingt, sich umfassende Zugriffs- und Administratorenrechte auf das jeweilige Zielsystem zu verschaffen. Somit wäre es ihnen in der Folge möglich, diese Rechte auszunutzen und etwa Sabotage oder Spionage zu betreiben. Ein tatsächlicher Missbrauch kann dabei jedoch nicht immer beobachtet werden.[22] Hijacking stellt in gewisser Weise eine (technische) Ergänzungskategorie zu Data Theft und/oder Disruption dar. So wird ein System zumeist gehijackt, um entweder Data Theft oder Disruption als eigentliches Ziel zu ermöglichen. Daher erfasst der HD-CY.CON Hijacking oft in Kombination mit Data Theft und/oder Disruption.

Jede der drei Angriffskategorien kann entweder mit ›1‹ oder ›2‹ hinsichtlich ihrer Intensität bewertet werden. Für Data Theft-Fälle erfolgt diese Unterscheidung anhand der Sensitivität/Vertraulichkeit der abgegriffenen Daten aus Sicht des Opfers. Im Datensatz wird somit nicht die technische Güte der Spionage-Operation, sondern die Klassifizierung der betroffenen Daten hinsichtlich ihrer Bedeutung für das betroffene Ziel als Indikator der Intensität verwendet. Je sensibler/vertraulicher die abgegriffenen Daten, desto schwerwiegender der Angriff. Da hierbei wiederum kein hartes Schwellenwertkriterium zur Anwendung kommen kann, beinhaltet die Kodierung in diesem Fall eine gewisse Interpretationserfordernis seitens des Kodierers oder der Kodiererin, sofern das Opfer selbst oder die jeweiligen Quellen keine eigene Einschätzung hinsichtlich des Vertraulichkeits-/Bedeutungsstatus der Daten liefern. Für staatliche AkteurInnen wird dabei zwischen ›non-classified‹ (1) und ›classified‹ (2) Informationen unterschieden, für private AkteurInnen dagegen zwischen ›non-sensitive‹ (1) und ›sensitive‹ (2) Informatio-

21 Watering Hole-Angriffe nutzen hierfür erstellte Fake-Websiten aus, um an die Zugangsdaten adressierter NutzerInnen dieser Seite zu gelangen. Living-Off-the-Land-Operationen missbrauchen zur Infizierung bzw. Ausführung der Schadsoftware bereits auf dem Zielsystem installierte Programme, Apps etc. (Watanabe und Schmitz 2021).

22 Wie Buchanan 2017 richtig feststellt, ist die Unterscheidung zwischen Cyberspionage und vorbereitender Sabotage (also dem Äquivalent ›Hijacking without misuse‹ im HD-CY.CON) äußerst schwierig, insbesondere für das Opfer selbst. Somit dient der technische Sophistizierungsgrad des Angriffes, die Art der verschafften Zugriffsrechte, sowie Kontextfaktoren wie die Charakterisierung des jeweiligen Zieles, als Indikatoren, um dennoch zu einer Bewertung kommen zu können. Dringen mutmaßlich staatliche AngreiferInnen beispielsweise in die Industrial Control Systeme (ICS) eines Stromversorgers und damit kritischer Infrastrukturen ein, ist dieser Fall plausibler als Hijacking (vorerst ohne Misuse) zu bewerten, denn als bloße Cyberspionage.

nen. Auch wenn ein Opfer die Bedeutung der abgegriffenen Daten bewusst herunterspielen könnte, ist dies im Falle fehlender Einschätzungen Dritter die einzige Grundlage für eine Kodierung. Eine bewusst verzerrte Darstellung der Güte der abgegriffenen Daten sollte somit stets in Betracht gezogen werden. Gerade für der Öffentlichkeit/Wählerschaft verpflichtete AkteurInnen oder Institutionen könnte ein solches Vorgehen jedoch zu noch höheren Kosten führen, falls diese Falschdarstellung letztlich doch öffentlich werden sollte.

Im Falle der Disruption-Kategorie wird anhand der zeitlichen Dauer der Funktionsstörung unterschieden. Mehrtägige und darüber hinaus andauernde Störungen werden mit ›2‹ kodiert, während lediglich mehrstündige DDoS-Angriffe mit ›1‹ bewertet werden.[23] Hijacking ohne Misuse wäre die erste Intensitätsstufe der dritten Angriffstyp-Kategorie, während Hijacking mit Misuse deren Steigerung darstellt und somit mit dem Code ›2‹ versehen wird.[24] Zusätzlich zu den jeweiligen Bewertungen des vorgefallenen Angriffstyps erfasst der HD-CY.CON potenzielle physische Auswirkungen in direkter Folge eines Cyberangriffes. Beispielhafte Fälle hierfür wären die Zerstörung der Zentrifugen durch Stuxnet sowie die Stromausfälle in der Ukraine 2015 und 2016 (Farwell und Rohozinski 2011; Brewster 2016b; Greenberg 2019b). Es reicht hierfür nicht aus, wenn etwa ein Computer in Folge eines Angriffes dauerhaft ausgeschaltet bleiben müsste, wenn dessen Hardware dennoch uneingeschränkt funktioniert und der Shutdown lediglich eine Maßnahme zur Eindämmung einer Malware darstellt.[25]

Anhand des Beispiels von Stuxnet soll die Intensitätsbewertung veranschaulicht werden: Die zutreffenden Angriffstypen in diesem Fall wären sowohl Disruption, da die normale Funktionserfüllung der betroffenen Industrial Control-Systeme (ICS) durch den Angriff gestört wurde, als auch Hijacking mit Misuse, da die umfassenden Zugriffsrechte im Sinne der Manipulation der Geschwindigkeit der Zentrifugen ausgenutzt wurden. Da die Störung der betroffenen Nuklearanlage in Natanz der Quellenlage zufolge zudem über mehrere Jahre andauerte, werden sowohl Disruption als auch Hijacking jeweils mit ›2‹ kodiert. Die Zerstörung der Zentrifugen als direkte Folge der Cyberoperation qualifiziert Stuxnet für eine Kodierung der Kategorie ›Physical Effects‹ größer null: Da es lediglich in Natanz zu solch einer zerstörerischen Wirkung durch Stuxnet kam, wird die räumliche Kategorie mit ›1‹ bewertet. Für die Dauer der Disruption wurde stattdessen eine ›2‹ kodiert, da diese länger als einen Tag andauerte. Insgesamt ergibt sich für Stuxnet somit ein ungewichteter Intensitätswert ›7‹. Der angesprochene Target-Multiplier 1,5 würde zudem greifen, da Einschätzungen von IT-Experten zufolge das iranische

23 Gerade im Falle von DDoS-Attacken, der häufigsten Disruption-Angriffsart, stellt die zeitliche Dauer den zumeist am ehesten zu bewertenden und damit konsistentesten Indikator für die Intensität des Angriffes dar.

24 In diesem Fall drückt sich der Misuse zumeist entweder durch Data Theft oder Disruption aus, weshalb hier mehrere Incident-Types vorliegen würden. Hijacking ohne Misuse kann das Infiltrieren fremder Systeme über einen längeren Zeitraum bedeuteten, wobei jedoch nach öffentlichem Kenntnissstand die erlangten Zugriffsrechte (bislang) noch nicht missbraucht wurden (vgl. Errichtung von »*beachheads*« in Zielsystemen, s. Buchanan 2017).

25 Ein Beispiel hierfür wäre die tausendfache Abschaltung von Computern innerhalb der saudi-arabischen Ölfirma Saudi Aramco, als Reaktion auf die Verbreitung der schadhaften Shamoon-Software 2012. Hierbei waren jedoch die ICS-Bestandteile der Ölförderung nicht betroffen (Perlroth 2012).

Atomwaffenprogramm in Folge von Stuxnet um bis zu zwei Jahre zurückgeworfen wurde (Katz 2010), was als Schwächung der offensiven Militärstrategie des Landes gewertet werden kann. Insgesamt ergibt sich somit ein gewichteter Wert von ›10,5‹ für Stuxnet, was bislang als eine Art Ausreißer in maximaler Richtung zu werten ist. Für den Großteil der zu kodierenden Angriffe werden allein aufgrund der nichtvorhandenen physischen Effekte sowie des wohl eher selten greifenden Target-Multipliers Werte zwischen eins und sechs erwartet.

Neben diesen technischeren Analysekriterien erfolgen nun die Beschreibung der Politisierungsmessung und eine Diskussion ihrer Relevanz für die Cyberkonfliktforschung.

4.2.1.3 Politisierung

Neben den Aspekten der Attribution und Intensität der erfassten Cybervorfälle stellt die Kodierung potenzieller Politisierungen einen weiteren Mehrwert des HD-CY.CON dar. Die Frage nach der politischen Adressierung von Cyberangriffen impliziert dabei mehrere theoretisch bedeutsame Komponenten: Zuerst bedeutet die Politisierung ein wichtiges Inklusionskriterium von Cyberoperationen ohne sonstige politische Dimension im Rahmen des Datensatzes. Rein auf finanzielle Gewinne ausgerichtete Cyberkriminalitätsvorfälle, die zudem weder auf ein politisches Ziel gerichtet noch einem politischen Akteur zugesprochen wurden, können und müssen im Falle einer Politisierung nichtsdestotrotz erfasst und kodiert werden, da ihnen durch diesen Akt eine politische Dimension verliehen wird (Steiger et al. 2018, S. 89). Zweitens können auch hier existierende Unterschiede zwischen den Regimetypen untersucht werden. Aufgrund des demokratischen Gebots transparenter Regierungspraxis sowie umfassender Kontrollbefugnisse nichtstaatlicher AkteurInnen ist von einem höheren Maß an Politisierungen von Cyberoperationen in demokratischen Staaten durch die jeweilige Regierung auszugehen als in ihren autokratischen Pendants (Steiger et al. 2018, S. 91). Darüber hinaus stellen sich jedoch weitere Fragen hinsichtlich staatlicher Politisierungspraktiken: Werden diese regelmäßig in besonderem Maße gegenüber bestimmten AngreiferInnen, z.B. ›Enduring Rivals‹, angewandt? Politisieren Regierungen in erster Linie Angriffe auf staatliche oder private Ziele im eigenen Inland? Inkludieren Politisierungen von Cyberoperationen sämtliche Incident-Types oder werden regelmäßig in erster Linie die disruptiveren Formen, etwa Hijacking mit Missbrauch, gepaart mit einer durch physische Schäden besonders hohen Intensität, politisiert? Und zuletzt: Sind es vor allem PolitikerInnen außerhalb der Regierung, die Politisierungen vornehmen, um den Handlungsdruck auf die Regierung in solchen Fällen zu erhöhen, auch hinsichtlich geforderter Attributionen?

4.2.1.4 Beschreibung der übrigen Kategorien des Datensatzes

Nachdem die zentralsten Kategorien des HD-CY.CON-Codebooks vorgestellt und theoretisch plausibilisiert wurden, erfolgt nun eine Zusammenfassung der übrigen Kategorien.[26]

26 Es werden hier wieder nur die inhaltlich bedeutsameren Kategorien vorgestellt, das gesamte Codebook findet sich bei Harnisch et al. 2021.

Die Kodierung der betroffenen Ziele erfolgt analog zur Erfassung des oder der Angreifer(s), somit werden diese in »*Receiver-Category*« sowie »*Receiver-Country*« unterschieden (Steiger et al. 2018: 82):

Tabelle 3: Kategorie ›Receiver-Category‹ HD-CY.CON

Code	Subcode	Beschreibung
0		Unknown
1		State-Institutions/Political System
	1	Government/Ministries
	2	Legislative
	3	Civil Service/Administration
	4	Judiciary
	5	Military
	6	Police
	7	Intelligence Agencies
	8	Political Parties
	9	Election-Infrastructure/Related Systems
	11	Other (e. g. Embassies)
2		International/Supranational Organization
3		Critical Infrastructure
	1	Energy
	2	Water
	3	Transportation
	4	Health
	5	Chemicals
	6	Telecommunications
	7	Food
	8	Finance
	9	Defence-Industry
4		Social Groups
	1	Ethnic
	2	Religious
	3	Hacktivist

	4	Criminal
	5	Terrorist
	6	Human-Rights-Organizations/Activists
	7	Political Opposition/Dissidents/Expats
	8	Other (e. g. NGOs with political goals)
5		Commercial Targets
6		End User(s)
7		Media
8		Science
9		Other

(Eigene Darstellung)
*Mehrfachkodierungen innerhalb eines Falles sind möglich, falls verschiedene Receiver-Categorys im Rahmen eines Angriffes betroffen waren (bis zu zehn Codes).

Entsprechend der verwendeten Konfliktdefinition des HIIK erfasst der HD-CY.CON (wenn möglich) nicht nur Informationen über Opfer, Täter, technische Ausgestaltung und Auswirkung des Angriffes, sondern auch, was die Täter zu ihrem Handeln veranlasst hat. Dieses ›Conflict-Issue‹ ist zentraler Bestandteil der allgemeinen Konfliktmessung des HIIK und sieht dabei folgende Kodieroptionen vor:

Tabelle 4: Kategorie ›Conflict-Issues‹ im HD-CY.CON

Code	Beschreibung
0	No Spillover
1	System/Ideology
2	National Power
3	Autonomy
4	Territory
5	Subnational Predominance
6	Resources
7	International Power
8	Decolonization
9	Secession

10	*(Nur Cyber-Conflict-Issue)*: Cyber-specific*
11	*(Nur HIIK Offline-Conflict-Issue)***: Third-Party-Intervention/Third-Party-Affection

*Im HIIK-Codebook nicht enthalten.
** Im HIIK Codebook nicht enthalten. Wird jedoch zusätzlich zum HIIK Offline-Konfliktgegenstand kodiert, wenn der auf der Cyberebene attackierende Akteur sich in seiner Handlung auf einen HIIK-Konflikt bezieht, bei dem er eigentlich kein Teil der Konfliktdyade ist. Beispiel: Türkische HackerInnen greifen Armenien als Reaktion auf Entwicklungen im Konflikt zwischen Armenien und Aserbaidschan um Bergkarabach an; daraus ergäbe sich folgende Kodierung der HIIK-Offline-Conflict-Issues: Siehe HIIK Konfliktbarometer Dyade Aserbaidschan – Armenien im Startjahr der Cyberoperation + 11.

Die in Tabelle 4 gelisteten Konfliktgegenstände werden jeweils für die Cyberoperation selbst sowie einen potenziell zugrunde liegenden Konflikt kodiert. Für die konventionelle Ebene wird zudem die Intensität der Konfliktdyade des betreffenden Konfliktbarometers im Cyberoperationsstartjahr erfasst. Grundlage hierfür ist jedoch, dass sich die Cyberoperation auch plausibel diesem konventionellen Konflikt und zumindest einem der dabei im Konfliktbarometer angegebenen Konfliktgegenstände zuordnen lässt. Die Kodierung dieses ›Cyber-Conflict-Issue‹ erfolgt entsprechend der vom HIIK aufgestellten Kategorien (Tabelle 4), sieht jedoch an zehnter Stelle die Zusatzkategorie ›Cyber-specific‹ vor. Diese wird kodiert, falls eine Konflikthandlung ohne die Existenz des Cyberspace nicht möglich bzw. nötig wäre. Ein Beispiel hierfür wären DDoS-Attacken seitens HacktivistInnen gegen eine Regierung, die zuvor Internetzensurmaßnahmen verhängt hat.[27]

Die Kategorie ›Zero-Days‹ gibt ferner an, ob Informationen über die Verwendung von einem (›2‹) oder mehreren (›2,1‹) Zero-Day-Exploits vorliegen. Wie bereits erläutert, werden diese speziellen Sicherheitslücken in erster Linie von sophistizierten, mit entsprechenden Ressourcen ausgestatteten AkteurInnen verwendet, da deren ›Finden‹ zumeist bereits eine Herausforderung darstellt (Steiger et al. 2018, S. 84). Somit kann über die Erfassung verwendeter Zero-Days eine Attribution potenziell gestützt oder auch zumindest in Zweifel gezogen werden. Nutzt beispielsweise eine APT, der staatliche Unterstützung nachgesagt wird, einen Zero-Day-Exploit im Zuge der Attacke, so könnte dies die Attribution stützen, da in erster Linie staatlichen Behörden und AkteurInnen deren Sammlung und Verwendung nachgesagt werden. Da diverse Zero-Days jedoch bereits länger im Internet kursieren,[28] aufgrund unzureichender Patching-Praktiken der AnwenderInnen der Zielsysteme jedoch immer noch erfolgreich ausgenutzt werden können, ist eine derartige Schlussfolgerung stets mit Bedacht zu ziehen, was im Rahmen dieser Arbeit nur in besonders plausiblen Fällen erfolgt.[29] Die Malware Stuxnet, bei der

27 In einem solchen Fall würde zusätzlich ›System/Ideology‹ als Cyber-Conflict-Issue kodiert werden.
28 Die gängige Bezeichnung hierfür lautet »*in the wild*« (Osborne 2020).
29 Das sog. »*Common Vulnerability Scoring System*« (Mell et al. 2007) stellt einen möglichen Indikator für die jeweilige Charakterisierung der Sicherheitslücken dar.

vier verschiedene, ›echte‹ Zero-Days ausgenutzt wurden, kann auch in diesem Fall als exemplarisch angesehen werden, da hierdurch die Attribution in Richtung amerikanischer und israelischer Geheimdienste untermauert wurde.

4.2.2 Allgemeine Kennzahlen zum Datensatz im Vergleich

Der HD-CY.CON zeichnet sich (wie in Tabelle 5 dargestellt) durch eine weitaus umfassendere Datenbasis aus als die beiden bekanntesten Alternativ-Datensätze. So verzeichnet er 1265 Cyberoperationen für die Jahre 2000–2019. Im Falle des DCID (1.5) sowie des CFR-Tracker sind es weitaus weniger erfasste Fälle, was sich teilweise aus dem engeren Fokus auf staatliche/staatlich gesponserte AngreiferInnen ergibt. Auch wenn der HD-CY.CON für Cyberoperationen mit staatlicher Beteiligung mit 512 erfassten Fällen unter der Zahl des CFR-Trackers liegt (siehe Abschnitt 5.2.1), bietet er dennoch insgesamt die umfassendere Datenbasis: So erfasst der HD-CY.CON aufgrund einer differenzierteren Attributionskodierung in anderen AngreiferInnen-Kategorien diverse Fälle, die vom CFR-Tracker als staatlich gesponsert erfasst wurden, etwa wenn die öffentliche Quellenlage entgegen der Kodierung des CFR-Trackers keine staatliche Unterstützung der Operation suggeriert.

Tabelle 5: Vergleich politikwissenschaftlicher Cyberkonfliktdatensätze

Datensatz	Zeitraum (Startjahr)	Erfasste Fälle*	Kodierintervall
HD-CY.CON	2000 – 2019	1265	Jährlich
DCID (1.5)	2000 – 2016	266	Unregelmäßig (mehrere Jahre)
CFR Tracker	2005 – 2020	541	Vierteljährlich

(Eigene Darstellung), *Stand: November 2021

4.3 Theoriegeleitete Fallauswahl mithilfe deskriptiver Statistik

Entsprechend eines ›sequenziell quantitativ-qualitativen‹ Designs folgt auf den quantitativen Untersuchungsteil im Sinne einer deskriptiven Auswertung des HD-CY.CON zur Durchführung der Fallauswahl ein strukturierter, fokussierter Vergleich als qualitativer Forschungsschritt (Kelle 2014, S. 161). Dabei wird die jeweilige Bedeutung der Forschungsteile gleich gewichtet (Kelle 2014, S. 160): Obwohl ein strukturierter Vergleich auch ohne die umfangreiche Auswertung eines Large-n-Datensatzes durchgeführt werden kann, wären seine Repräsentativität und Validität im Sinne der Fallauswahl begrenzt. Der HD-CY.CON-Datensatz reduziert somit empirische ›blinde Flecken‹, die die Fallauswahl verzerren könnten. Die Kombination aus quantitativer Häufigkeitsanalyse und qualitativ strukturierter, vergleichender Analyse soll dazu dienen, die vermutete Beziehung zwischen Regimetyp und Proxy-Nutzung in einem bislang unterentwickelten Forschungsgebiet ohne ausreichende Grundlagenforschung zu untersuchen (Kelle

2014, S. 153). Dies gilt noch stärker für die konzeptualisierte defensive Cyberproxy-Nutzung demokratischer Staaten.

Nach der statistischen Beschreibung des Datensatzes werden jeweils zwei Fälle für Autokratien und Demokratien ausgewählt: Unter einem ›Fall‹ werden im Kontext der Arbeit ein Land und dessen Proxy-Nutzung/Beziehung im Untersuchungszeitraum verstanden. Für die Gruppe der Autokratien sollen somit Varianzen in Art und Funktion der prävalenten Proxy-Nutzung aufgezeigt und erklärt werden.[30] Daher gilt es, zwei besonders häufig und intensiv Cyberproxys nutzende Autokratien aus dem Datensatz herauszufiltern, denen dennoch zusätzlich eigene staatliche Cyberangriffe zugesprochen wurden, um den potenziellen Aspekt der Plausible Deniability als primäres Motiv zur Proxy-Nutzung noch stärker untersuchen zu können.[31] Zweitens können somit auch zeitliche Varianzen in der Proxy-Nutzung gegenüber allgemein/direktstaatlich attribuierten Cyberoperationen eher identifiziert werden, was beispielsweise auf die bewusste Entmachtung einer staatlichen Institution durch die zeitweilige Instrumentalisierung von Proxys hindeuten könnte.

Die beiden Autokratien sollten hinsichtlich der anvisierten Ziele der Angriffe, der angewandten Incident-Types sowie des autokratischen Subtyps regelmäßige Unterschiede aufweisen. Darüber hinaus ist eine möglichst große zeitliche Abdeckung des Datensatzes seitens der Länder erstrebenswert: Je mehr Daten für die ausgewählten Autokratien vorliegen, desto fundierter können die anschließenden Fallstudien wiederum durch den HD-CY.CON gestützt werden. Durch die exemplarische Analyse besonders häufig eingesetzter Proxy-Gruppierungen kann somit im vergleichenden Untersuchungsdesign die bereits im Datensatz angelegte Längsschnittkomponente im Sinne einer potenziellen ›Within-Case-Variance‹ noch expliziter analysiert werden (Levy 2008, S. 10). Für die abhängigen Variablen des Analysemodells steht somit im Kontext der Fallauswahl der Aspekt der Funktion der Proxys notwendigerweise zunächst im Vordergrund, da dieser im Gegensatz zur Art direkt aus dem Datensatz abgelesen werden kann. Nichtsdestotrotz wird bei der Fallauswahl auch darauf geachtet, ob die beiden favorisierten Autokratien hinreichende Unterschiede hinsichtlich ihrer Involvierung in gewaltsame konventionelle Konflikte und somit der Ausprägung der IV aufzeigen, wie sie der HD-CY.CON im Rahmen der HIIK-Offline-Issue/Intensity-Kategorien erfasst.

---

30 Somit soll aus methodologischer Sicht ein »*no-variance-design*« hinsichtlich der beiden AVs vermieden werden (King et al. 1994, S. 128–139). Eine vorhandene offensive, respektive defensive Cyberproxy-Nutzung wird jedoch als Voraussetzung für die Fallauswahl angenommen, »*variance*« bedeutet hier somit *nicht* die dichotome Konstellation ›Cyberproxy-Nutzung‹ vs. ›keine Cyberproxy-Nutzung‹.

31 Allgemein/direktstaatlich attribuierte Cyberoperationen der beiden Autokratien dienen somit in gewisser Weise als Kontrollfälle, um das autokratische Grund-Motiv für offensive Cyberproxy-Nutzung im Generellen systematischer für den jeweiligen Fall herausarbeiten zu können. Würden nur Autokratien mit ausschließlich kodierten Proxy-Operationen untersucht werden, könnten die Motive der Plausible Deniability, sowie des Coup Proofings nicht hinreichend auf ihre Erklärungskraft getestet werden, da in solchen Fällen fehlende staatliche Kapazitäten zur Durchführung eigener Cyberoperationen am plausibelsten erscheinen (unter der Bedingung eines grundlegenden Interesses hieran) und die beiden anderen genannten Motive, wenn, dann eher als Sekundärmotive einzustufen wären.

Auf demokratischer Seite kann, wie bereits beschrieben, eine Fallauswahl aufgrund der US-amerikanischen Suprematie im Technologiesektor eigentlich nur über die Vereinigten Staaten als ›Most-Likely-Case‹ erfolgen. Entsprechend der Auswertung des HD-CY.CON soll jedoch überprüft werden, ob es andere Demokratien gibt, die bereits ähnliche Proxy-Nutzungspraktiken demonstriert haben. Denkbar wären hier etwa Großbritannien und Israel aufgrund ihrer Stärke im privatwirtschaftlichen IT-Sektor. Die am zweithäufigsten durch nationale IT-Firmen attribuierende Demokratie des Datensatzes wird somit den USA als Vergleichsfall zur Seite gestellt. Ist deren Attributionshäufigkeit des IT-Sektors im Gegensatz zu den nachfolgend platzierten Demokratien vergleichsweise gering, wird als weiteres Kriterium die Anzahl an erfassten IT-Unternehmen ausgewählt. Für einen hinreichend geeigneten Vergleichsfall mit den USA erscheint z.B. ein Land mit nur einer im Datensatz vertretenen IT-Firma weniger geeignet als ein Land mit größerer Diversität in diesem Bereich.

Ließen sich außer für die USA keine derartigen Attributionsmuster auf Seiten einer weiteren Demokratie erkennen, läge die Vermutung nahe, dass es sich bei der konzeptualisierten defensiven Cyberproxy-Nutzung eher um eine US-spezifische Anomalie als um ein allgemein demokratisches Phänomen handeln könnte. Im Falle demokratischer Cyberproxy-Nutzung wird an dieser Stelle deutlich, dass die im Rahmen der Arbeit durchgeführte Konzeptualisierung durch weniger theoretische sowie empirische Vorarbeiten gestützt wird als im Falle klassischer, autokratischer Cyberproxy-Nutzung. Somit kommt der Fallauswahl auf demokratischer Seite eine etwas andere Rolle zu als auf autokratischer Seite. Für Autokratien erscheint die These der offensiven Cyberproxy-Nutzung bereits vor der Analyse als wahrscheinlich, daher wird hier der Fokus auf Varianzen innerhalb der jeweiligen Strategie (AVs) gelegt. Im Falle der Demokratien gilt es hingegen, zunächst die These der defensiven, attributionsbasierten Proxy-Nutzung *per se* zu überprüfen. Etwaige Varianzen innerhalb dieser stellvertretenden Attributionen sollen dagegen stärker im Laufe der empirischen Analyse herausgearbeitet und für eine potenzielle Anpassung der Ursprungshypothesen genutzt werden. Ein weiterer demokratischer Vergleichsfall, dessen Attributionskodierungen ebenfalls auf eine defensive Cyberproxy-Nutzung schließen lassen, könnte somit das theoretische Argument erhärten bzw. im Hinblick auf potenzielle, intrademokratische Varianzen weiter ausdifferenzieren und somit zur Weiterentwicklung des Erklärungsmodells beitragen.

Konkret wird zunächst auch aufseiten der Demokratien durch Zuhilfenahme deskriptiver Statistik ermittelt, ob die getätigten Hypothesen bezüglich einer grundlegend niedrigeren bis kaum vorhandenen offensiven Proxy-Nutzung im Cyberspace auf Grundlage der Daten zu bestätigen sind. Ist dies der Fall, wird für die propagierten, defensiveren demokratischen Cyberproxys eine Häufigkeitsanalyse der kodierten Länder, aus denen die jeweils attribuierenden IT-Firmen stammen (Variable ›Country of Origin: IT-Attribution‹), vorgenommen. Verglichen werden die beiden am häufigsten kodierten Länder sodann mit den in den betreffenden Fällen kodierten Receiver-Countrys. Um als relevanter Fall auf demokratischer Seite gelten zu können, müssten hierbei regelmäßige Übereinstimmungen zu finden sein.

Tabelle 6 verdeutlicht die Schwerpunktlegung auf die variante Ausprägung der AVs im Falle der Autokratien sowie die zunächst dichotom positive Ausprägung der AVs im Falle der Demokratien mit dennoch potenziell herauszuarbeitenden Varianzen.

Tabelle 6: Schematische Darstellung des Vorgehens der Fallauswahl

	AV I	AV II	UV	KV	IV
Autokratien	*Positiv/Varianz*	*Positiv/Varianz*	*?*	*?*	*?*
Demokratien	*Positiv/Varianz möglich*	*Positiv/Varianz möglich*	*?*	*?*	*?*

(Eigene Darstellung)

4.4 Konzeptoperationalisierung im Rahmen eines strukturiert-fokussierten Vergleiches

Der angestrebte Ansatz des »*structured-focussed comparison*« (SFC) wird seitens seiner Entwickler George und Bennett wie folgt beschrieben:

> »The method and logic of structured, focused comparison is simple and straightforward. The method is ›structured‹ in that the researcher writes general questions that reflect the research objective and that these questions are asked of each case under study to guide and standardize data collection, thereby making systematic comparison and cumulation of the findings of the cases possible. The method is ›focused‹ in that it deals only with certain aspects of the historical cases examined. The requirements for structure and focus apply equally to individual cases since they may later be joined by additional cases.« (George und Bennett 2005, S. 67)

Der gewählte Ansatz lässt sich somit ebenfalls als theoriegeleitetes Process-Tracing im Rahmen eines Small-n-Vergleiches beschreiben. Auch wenn keine vergleichbare Generalisierbarkeit wie im Falle statistischer Large-n-Untersuchungen erreicht werden kann, erlaubt dieses Vorgehen durch die erreichte Analysetiefe die Bewertung komplexer kausaler Prozesse, da dies in stetiger Verbindung mit den theoretisch hergeleiteten Annahmen erfolgt (Hall 2003, 391–392). Die genuinen Charakteristika des Cyberspace, z. B. das hohe Maß an Geheimhaltung und verdeckten Operationen sowie das allgemein eher geringe Maß an politischer Transparenz, erfordern eine qualitative Untersuchung der beschriebenen UV, IV und KV. Dagegen können die AVs durch den HD-CY.CON hinsichtlich der Fallauswahl statistisch erhoben und ausgewertet werden. Jedoch gebietet auch bei ihnen die nachgelagerte Bewertung der jeweils fallbezogenen Ausprägungen die Anreicherung durch qualitativ erhobene Indikatoren zur umfassenden Beschreibung der Proxy-Funktionen und -Typen.

Im Rahmen des SFC folgt der/die WissenschaftlerIn folgenden fünf Arbeitsschritten (Bennett 2004, S. 32–33):

1. Spezifizierung der Forschungsfrage,
2. Definieren der UV, AV und IV,
3. Auswahl und Vergleich der Fallstudien,

4. Operationalisierung der Variablen-Ausprägungen sowie
5. Formulieren der jeweils strukturierenden Forschungsfragen.[32]

Die Schritte 1 und 2 wurden bereits in den vorherigen Kapiteln durchgeführt und beschrieben.[33] Da die Auswahl und der Vergleich der Fallstudien erst nach der Analyse des HD-CY.CON erfolgen können, gilt es nun, die Variablen des Kausalmodells zu operationalisieren und anschließend die Forschungsfragen für die Fallstudien zu formulieren. Bei der Operationalisierung der Konzepte der zu untersuchenden Variablen sollen entsprechend des ontologischen Ansatzes von Gary Goertz neben theoretischen Erwägungen auch empirische Beobachtungen in die Spezifizierung einfließen. Nur so könne verhindert werden, dass Konzeptdefinitionen und deren empirische Analyse einzig nach Belieben der jeweilig gewählten Definition des Forschers willkürlich konstruiert werden. Die zentralen Attribute eines Konzeptes seien somit jene, die besondere Relevanz für deren Verwendung und Analyse im Rahmen von Hypothesen und Kausalmodellen aufweisen (Goertz 2012, S. 4). Dies stellt zudem den Nexus zur Analyseeinheit der »*causal-process observations*« (CPOs) her, »*an insight or piece of data that provides information about context, process, or mechanism, and that contributes distinctive leverage in causal inference*« (Collier et al. 2004, S. 252). Somit werden nicht nur standardisierte »*data-set observations*« (DSOs) des HD-CY.CON analysiert (Collier et al. 2004, S. 252), sondern auch nicht standardisierbare CPOs, die dennoch einen hohen Nutzen im Rahmen des Process-Tracings besitzen (Mahoney 2010, S. 127).

4.4.1 Funktionen autokratischer Cyberproxys

Gemäß der Verwendung des HD-CY.CON werden die verschiedenen *Funktionen* (AV I) und somit die Zwecke des autokratischen Cyberproxy-Gebrauchs in erster Linie über den jeweils angewandten Incident-Type im Rahmen offensiver Cyberoperationen operationalisiert (Data Theft, Disruption, Hijacking; siehe 4.2.1.2). Jedoch kann etwa Datendiebstahl ökonomisch, militärisch oder politisch motiviert sein und somit unterschiedliche Funktionen für den staatlichen Auftraggeber erfüllen. Entscheidend wäre für die Funktionsbeurteilung, das Profil der Ziele sowie (falls öffentlich bekannt) der abgegriffenen Daten zu kennen. Die genaue Identität der Täter (AV II) kann darüber hinaus weitere Anhaltspunkte für die Bewertung der intendierten Funktion des Proxy-Einsatzes liefern. So könnte etwa die Infiltration kritischer Infrastrukturen seitens militärisch geführter Proxys als Vorbereitung eines Sabotageaktes (Hijacking plus Misuse) im Rahmen eines konventionellen Konfliktes interpretiert werden, während dasselbe Vorgehen von zivilgeheimdienstlich geleiteten Proxys in Abstinenz eines konventionellen Konfliktes lediglich

32 »These questions must be carefully developed to reflect the research objective and theoretical focus of the inquiry. The use of a set of general questions is necessary to ensure the acquisition of comparable data in comparative studies. […] The important device of formulating a set of standardized, general questions to ask of each case will be of value only if those questions are grounded in – and adequately reflect – the theoretical perspective and research objectives of the study« (George und Bennett 2005, S. 69).

33 Als ›class of events‹ wäre im Rahmen der Arbeit staatliche Cyberproxy-Nutzung zu verstehen.

als allgemeine Aufklärungstätigkeit gewertet werden könnte. Disruption kann dagegen ein allgemeines Signalisieren der eigenen Fähigkeiten oder eine zielgerichtete Maßnahme im Rahmen eines konventionellen Konfliktes darstellen.

In der Literatur wird an dieser Stelle oftmals kritisch vermerkt, dass die tatsächliche Intention von CyberangreiferInnen nur schwer zu beurteilen und diese Bewertung anfällig für menschliche Fehlschlüsse ist (Libicki 2018, S. 118). Der letztliche Zweck von Datendiebstahl ist hierfür das prägnanteste Beispiel. In dieser Arbeit wird jedoch argumentiert, dass gewisse Muster bzw. Varianzen in der faktisch sichtbaren Anwendung von Proxys im Zeitverlauf dennoch Hinweise darauf sein können, welche Funktionen und Ziele hiermit erreicht werden sollten. Ändert eine Autokratie ihre Cyberproxy-Nutzung beispielsweise aufgrund einer erfolgten Eskalation in Folge einer Infiltrierung kritischer Infrastrukturen, so kann dies als Zeichen gewertet werden, dass das eigene Entdeckt werden nicht Teil des ursprünglichen Plans war, sondern dass in erster Linie Informationen gesammelt werden sollten. Wird eine Autokratie dagegen bei einem solchen Vorgehen in Gestalt ihres Proxys überführt, nutzt denselben Akteur jedoch auch in der Folge auf ähnliche Zielsysteme, kann von einem intendierten Signaling-Effekt der eigenen Fähigkeiten ausgegangen werden, ohne diese notwendigerweise auch final zur Anwendung bringen zu müssen.[34] Ob der tatsächliche Missbrauch der Zugriffsrechte zu einem Zeitpunkt tatsächlich geplant war, kann dabei ohne Insider-Kenntnisse nur schwer beurteilt werden. Wahrscheinlicher erscheint dies jedoch, falls sich die Autokratie mit dem jeweiligen Land bereits in einem gewaltsamen konventionellen Konflikt befindet oder sich dieser zumindest bereits andeutet.

Zusammenfassend dient als Hauptindikator für die autokratischen Cyberproxy-Funktionen deren jeweils angewandter Incident-Type, der jedoch im Sinne einer kontextuellen Attribution zu den jeweils anvisierten Zielen sowie den attribuierten AkteurInnen in Beziehung gesetzt werden muss.

4.4.2 Arten autokratischer Cyberproxys

Die institutionelle Anbindung autokratischer Cyberproxys bzw. deren Art kann dagegen aus dem HD-CY.CON über die Kategorie ›Name-Initiator‹ operationalisiert werden. Darin werden sowohl potenzielle Bezeichnungen der attribuierten AngreiferInnen als auch bekannte Affiliationen zu konventionellen Akteuren, etwa zu dahinter vermuteten Unternehmen, aber vor allem auch staatlichen Einheiten, kodiert.[35] Hierüber können Aussagen über die Häufigkeit der jeweils vermuteten institutionellen Anbindung offensiver Cyberproxys erfolgen, die jedoch für eine umfassende Bewertung durch qualitative Primär- und Sekundärquellen ergänzt werden müssen. Diese können Aufschluss darüber liefern, welchem Teil der Winning Coalition sich einzelne staatliche Einheiten zuordnen lassen und inwiefern sich deren strategische Eigeninteressen sowie ihr Herrschaftszugang über die Zeit verändert haben könnten. Sofern es die Datenlage zulässt,

34 Zudem impliziert dieser Fall, dass die entsprechende Attributionspraxis des betroffenen Staates dessen Verwundbarkeit gegenüber dem autokratischen Cyberangreifer offensichtlich nicht effektiv reduziert hat, im Falle einer erfolgreichen Infiltration.

35 Beispiel: Name Initiator I: Charming Kitten; Name Initiator II: IRG (iranische Revolutionsgarden).

soll zusätzlich eine Bewertung einzelner Cyberoperationen entsprechend des Analyserasters zu staatlicher Verantwortlichkeit im Cyberspace von Jason Healey (2011) vorgenommen werden, die durch den HD-CY.CON in ihrer Granularität nicht erfasst werden kann (2011, S. 59–61):

Tabelle 7: Das Spektrum staatlicher Verantwortlichkeit im Cyberspace

Kategorie*	Beschreibung
State-ignored	Der Staat weiß von den Aktivitäten privater AkteurInnen, lässt diese jedoch gewähren.
State-encouraged	Der Staat liefert privaten AkteurInnen ideelle/rhetorische Unterstützung, billigt deren Aktionen und ruft zu Nachahmungen auf.
State-shaped	Der Staat liefert privaten AkteurInnen informelle Unterstützung, etwa durch die Koordination mit gleichgesinnten AkteurInnen innerhalb der Regierung, die außerhalb ihrer Dienstzeit ähnliche Hacks ausführen.
State-coordinated	Der Staat unterstützt private AkteurInnen durch die Auswahl der Ziele, der zeitlichen Abläufe sowie operativer Details. Auch technische Unterstützung ist möglich.
State-ordered	Der Staat unterstützt private AkteurInnen vollumfänglich, ohne diese bereits de facto zu StaatsagentInnen gemacht zu haben.
State-rogue-conducted	Staatliche AkteurInnen führen ohne das Wissen oder gegen den Willen der Regierung Cyberaktionen durch.
State-integrated	Private AkteurInnen werden in staatliche Cybereinheiten integriert. Die Befehle und Koordination können dabei formell oder informell sein, jedoch hat der Staat stets die Kontrolle über die Zielauswahl sowie die operativen Details.
State-executed	Staatliche Cybereinheiten führen Cyberoperationen unter direkter Kontrolle der staatlichen Führung durch.

Quelle: Jason Healey (2011, S. 59–61)
*Es werden hier nur acht der insgesamt zehn Kategorien ausgewählt, da die beiden passivsten Verantwortungsformen (›state-prohibited‹ und ›state-prohibited but inadequate‹) dem hier verwendeten Proxy-Konzept nicht mehr entsprechen.

4.4.3 Funktionen demokratischer Cyberproxys

Aufgrund der zentralen Funktion defensiver Cyberproxys im Sinne der Attribution können auf demokratischer Seite Varianzen standardisierter DSOs nur eingeschränkt direkt aus dem Datensatz herausgelesen werden, weshalb hier CPOs von noch zentralerer Bedeutung sind. So zeigte die Konzeptualisierung der demokratischen AV I, dass auch die spezifischere Funktion technischer Attributionen variieren kann. Entsprechend der diskutierten Legitimations- und Resilienzfunktionen sowie dem allgemeinen Ziel der Reduzierung politischen Handlungsdrucks stellvertretender Attributionen soll vor allem deren Beziehung zu entweder nicht vorhandenen oder zeitlich vor- oder nachgelagerten

politischen Attributionen untersucht werden. Hierfür sind als Indikatoren vor allem die HD-CY.CON-Kategorien ›Source-Incident-Detection/Disclosure‹, ›Temporal Attribution-Sequence‹ sowie die bereits erwähnten ›Attribution-Basis‹ und ›Attribution-Type‹"[36] dienlich. Erstere gibt dabei an (falls möglich), durch welchen Akteur der jeweilige Vorfall in erster Instanz öffentlich gemacht wurde, unabhängig von einer Attribution. So könnte eine gehäufte Kodierung von IT-Firmen für eine angestrebte Resilienzfunktion sprechen, die mit ihren technischen Berichten einhergeht. Die zweite Kategorie reflektiert dagegen, in welcher Reihenfolge die Attributionen im Falle sowohl vorliegender technischer als auch politischer Attributionen erfolgt sind. Dies könnte somit ein Hinweis darauf sein, ob a) demokratische Regierungen tatsächlich regelmäßig auf private Attributionen bauen, um zunächst den eigenen Handlungsdruck zu reduzieren, b) zuerst veröffentlichte IT-Berichte eine nachgelagerte, politische Attribution ohne umfangreiches Offenlegen eigener Evidenzen ermöglichen, oder c) zuerst erfolgte politische Attributionen durch nachgelagerte technische Attributionsberichte mehr Glaubwürdigkeit erlangen können.[37]

4.4.4 Arten demokratischer Cyberproxys

Die Operationalisierung der Art demokratischer Cyberproxys (AV II) ergibt sich dagegen entsprechend ihrer Konzeptualisierung aus der Erfassung der Kategorie der ›Attribution-Basis‹ sowie des ›Country of Origin: IT-Attribution‹ in Kombination mit dem jeweiligen ›Receiver-Country‹ und bedarf dementsprechend an dieser Stelle keiner weiteren Ausführung.

4.4.5 Domestische Präferenzkonstellationen

Die Operationalisierung der domestischen Präferenzkonstellationen als Haupterklärungs-variable für außenpolitisches Handeln im neuen Liberalismus gestaltete sich bislang relativ wenig formalisiert und divers, eine Art ›Goldstandard‹ scheint noch nicht zu existieren. Erklären lässt sich dies jedoch vor allem auch durch ihre Varianz von Land zu Land und besonders von Regimetyp zu Regimetyp, entsprechend des aufgezeigten Einflusses der republikanischen Ebene sowohl auf den Herrschaftszugang domestischer AkteurInnen als auch auf den konkreten Transfer ihrer Interessen auf die politische Ebene. Dass dabei auch autokratische Subtypen wie Einparteien-Regime wegen grundlegender Ähnlichkeiten zu Demokratien auf der republikanischen Ebene dieselben Kooperationsanreize im wirtschaftlichen Bereich wie diese besitzen können, verdeutlicht nochmals die Interdependenz der drei Liberalismus-Stränge (Mattes und Rodríguez 2014). Prinzipiell sind für die Operationalisierung der UV besonders die

36 In ihrer Dissertation von 2021 identifiziert auch Lee vier unterschiedliche »*channels*« der bisherigen US-Attribution (»*technical, criminal, official and unofficial policy*«), die ebenfalls auf die Differenzierung unterschiedlicher Attributionstypen abzielen.

37 Da die defensive Cyberproxy-Nutzung per se und somit auch besagte potenzielle Varianzen hierbei als weniger »*certain*« (Rohlfing 2014, S. 609) angesehen werden als im Falle autokratischer Cyberproxy-Nutzung, werden sie wie bereits beschrieben für die demokratische Fallauswahl auch als nicht zwingend notwendig erachtet.

Interessen von »*politicians, bureaucrats, organized interests, think tanks, NGOs, and voters*« von Bedeutung (da Conceição-Heldt und Mello 2016). Für die Erklärung des außenpolitischen Handelns wird es somit im ersten Schritt wichtig sein, herauszuarbeiten, welche dieser AkteurInnen durch ihren Herrschaftszugang auf republikanischer Ebene im jeweiligen Untersuchungszeitraum für das autokratische oder demokratische Land als besonders relevant erachtet werden können. In der Folge gilt es aufzuzeigen, zu welchen Präferenzkonstellationen gegenüber dem autokratischen oder demokratischen Gegenüber deren Interessen letztlich auf außenpolitischer Ebene führten bzw. geführt hätten, sofern durch den Einsatz des jeweiligen Cyberproxys diese potenzielle Verwundbarkeitsasymmetrie nicht zum eigenen Vorteil hätte gestaltet werden können/sollen. Die republikanische Ebene determiniert somit, welche ideellen und kommerziellen Interessen welcher AkteurInnen sich überhaupt auf politischer Ebene durchsetzen können. Für Demokratien wird aufgrund des zumindest in der Theorie funktionierenden Transmissionsriemens von einer größeren Vielfalt an potenziell hierfür in Frage kommenden AkteurInnen ausgegangen, abhängig vor allem auch vom jeweiligen Zeitkontext. So dürften WählerInnen im Wahlkampfzeitraum einen stärkeren Herrschaftszugang besitzen als kurz nach einer Wahl. Für Autokratien werden in erster Linie die jeweiligen Mitglieder der Winning Coalition und deren Präferenzen als zentral angesehen. Jedoch bedingt der autokratische Subtyp auch hier eine regelmäßige Varianz der Interessensdurchsetzungen unterschiedlicher Elitengruppen.

Auf demokratischer Seite gilt es somit noch stärker aufzuzeigen, welche Interessen welcher domestischen AkteurInnen für die seitens der Autokratie anvisierten Vulnerabilitätsasymmetrie in erster Linie verantwortlich gemacht werden können. Durch das Aufbrechen des Three-Image-Paradigmas der internationalen Beziehungen wird im neuen Liberalismus zudem der Einfluss von Dynamiken und Prozessen der internationalen Ebene auf diese domestischen Präferenzkonstellationen nachgezeichnet.[38] Diese könnten wiederum im Falle von Demokratien durch den in Folge einer Wahl veränderten Herrschaftszugang der AkteurInnen auf politischer Ebene gewandelte Präferenzen auf ideeller und/oder wirtschaftlicher Ebene nach sich ziehen.

Für die Analyse ideeller Präferenzen werden Primärquellen, z.B. staatliche Strategiepapiere, White Paper, Pressemitteilungen oder sonstige Äußerungen der jeweiligen Regierung bzw. bestimmter Teile der Winning Coalition als Indikatoren herangezogen, die über die Wertvorstellungen einer bestimmten Akteursgruppe Auskunft geben.[39] Stellungnahmen in Medienartikeln spielen jedoch auch eine bedeutende Rolle. Hinzu kommt die Analyse von Sekundärliteratur, in der bereits eine umfassende Auseinandersetzung mit der Analyse staatlicher Präferenzentwicklung auf (u.a.) ideeller Ebene für verschiedene Staaten stattfand. Für das Nachzeichnen wirtschaftlicher Präferenzen

38 Bedeutend ist in diesem Kontext auch der Effekt der »*social embeddedness*«, die »*may take the form of fixed investments by private firms, ideological commitments by political parties concerned about their reputation, costly institutional adaptation by domestic bureaucracies, or government investment in military defense*« und somit durch soziale »*lock-in*«-Effekte zu stabilen, staatlichen Präferenzen führen könne (Moravcsik 1997, S. 537).

39 Für cyber-spezifische Präferenzen könnten hierfür auch die dominanten und zunehmend veröffentlichten Cybersicherheits-Doktrinen auf staatlicher Ebene erfasst werden (Lewis 2014).

können dagegen auch stärker quantitative Messzahlen erfasst werden, die beispielsweise die wirtschaftspolitischen Tendenzen eines Landes sowie der darin dominanten AkteurInnen widerspiegeln. Aber auch allgemeine Verschiebungen innerhalb der Haushaltsentwürfe nationaler Regierungen können entsprechend des Prinzips ›Money is Policy‹ als mögliche Indikatoren für veränderte Präferenzkonstellationen in bestimmten Bereichen herangezogen werden (Adams und Williams 2010, S. 1).

Zuletzt wird der Einfluss der republikanischen Ebene besonders durch Bewertungen der verfassungsrechtlichen, institutionalistischen Strukturen des jeweiligen Landes im Untersuchungszeitraum erfasst. Ebenfalls wird erhoben, welche Varianzen darin zum Erstarken bestimmter AkteurInnen und deren Präferenzen geführt haben. Da in der vorliegenden Arbeit der autokratische und demokratische Subregimetyp als Teile der Konzeptualisierung der UV begriffen werden, werden diese wie folgt für die empirische Analyse operationalisiert:

Zur Konzeptualisierung autokratischer Subregimetypen wird die Typologie von Kailitz (2013) herangezogen: Dessen Ansatz liegt dabei die Frage nach der jeweiligen Legitimationsquelle autokratischer Regime für deren Ausdifferenzierung zugrunde. Die Unterscheidung zwischen liberalen Demokratien, elektoralen Autokratien, kommunistischen Ideokratien, Einparteien-Autokratien, Militärregimen, Monarchien und personalistischen Autokratien wird für das Forschungsinteresse der Arbeit aus zwei Gründen als besonders geeignet erachtet: Erstens sind hierdurch feingliedrigere Unterscheidungen hinsichtlich des Einflusses des Subregimetypus auf die republikanische sowie ideelle Ebene domestischer Interessenskonstellationen möglich. Wie Geddes et al. 2014 feststellten, entscheidet nicht nur die bloße Größe der Winning Coaltion/Leadership-Group über deren Handeln, sondern neben diesem formal-republikanischen Charakteristikum auch deren jeweilige Interessenslage. Somit sollten bei der Betrachtung unterschiedlicher autokratischer Subtypen nicht nur Weite und Enge des jeweiligen Herrschaftszugangs betrachtet werden, sondern auch deren Interessen auf ideeller sowie wirtschaftlicher Ebene, was gleichzeitig den Subregimetyp als Teil der UV begründet. Den Aspekt der Legitimation als Hauptunterscheidungskriterium zu wählen, ermöglicht dabei zweitens, die in Abschnitt 2.2.3 aufgezeigten Asymmetrien im autokratischen Herrschaftszugang nach innen und außen enger an die unterschiedlichen Subtypen anzubinden. Wie bereits diskutiert wurde, unterscheiden sich Autokratien besonders in ihrem Modus der eigenen längerfristigen Interessensdurchsetzungschancen gegenüber der domestischen, aber auch außenpolitischen Ebene. Da für den Cyberspace hierbei der Aspekt der Legitimation als immer bedeutsamer charakterisiert wurde, sollte die Konzeptualisierung autokratischer Regimetypen diesen theoretischen Aspekt auch entsprechend abbilden. Das Konzept der Legitimation ist zudem im Gegensatz zu den weiteren Säulen autokratischer Stabilität (Kooptation und Repression) anschlussfähiger an alle drei Liberalismus-Spielarten, da Legitimation auf unterschiedliche Weise generiert werden kann.[40]

40 Zum einen auf der Output-Ebene, etwa durch wirtschaftliche oder militärische Erfolge, oder aber auf der Input-Ebene, beispielsweise durch das Fördern eines Personenkults um den autokratischen Führer, oder aber einer allgemein nationalistisch-patriotischen Legitimierung der Regierung.

Das oberste Ziel autokratischer Regime ist die Sicherung der eigenen Stellung an der Spitze des defizitären bzw. verkürzten Transmissionsriemens im politischen Prozess. Da hierfür der Säule der Legitimation eine immer größere Bedeutung zugeschrieben wird, eignet sich eine solche Regimetypen-Klassifizierung auch besonders für die liberal geprägte Erfassung des Einflusses unterschiedlicher Legitimations- und somit Interessensdurchsetzungsstrategien nach innen und außen. Die Anwendung der gröberen Unterscheidung von Geddes (1999) würde vor allem auf republikanischer und ideeller Ebene zu viele bedeutsame Unterschiede autokratischer Subtypen sowie deren konditionierenden Einfluss der gesellschaftlichen Präferenzkonstellationen nicht erfassen.

Zur Unterscheidung demokratischer Subtypen wird zwischen liberalen und illiberalen Demokratien unterschieden, bei Letzteren liegt der Fokus jedoch auf der populistisch geprägten Variante. Während erstere sich verpflichten, ihre liberalen Norm- und Wertvorstellungen auch auf die tägliche Arbeit in den demokratischen Institutionen zu übertragen, besonders im Hinblick auf den Aspekt der Rechtsstaatlichkeit, unterhöhlen letztere die ursprünglich liberalen demokratischen Institutionen durch deren gesetzlich gedeckte Modifizierung.[41] Liberale Demokratien unterscheiden sich somit von ihrer illiberalen Variante insofern, als sie demokratische Institutionen, Regeln und Prinzipien nicht regelmäßig zu ihren Gunsten ausnutzen und die republikanische Ebene somit die liberal-demokratischen Identitäten des Landes weitgehend widerspiegelt. Illiberale Demokratien weisen dagegen Defizite in einem Teilbereich oder mehreren Teilbereichen des Modells der sog. »*Embedded Democracy*« auf (Merkel 2004).[42] Hierzu kann es, wie im Falle Ungarns unter Viktor Orban, kommen, wenn eine demokratische Regierung zunehmend illiberale Präferenzen entwickelt und demokratische Institutionen und Prinzipien für deren Durchsetzung politisch ausnutzt. Dies erschwert GegnerInnen der illiberalen Regierungshaltung, legitime politische Forderungen stellen und durchsetzen zu können, da deren Herrschaftszugang durch die entsprechenden rechtlichen Anpassungen signifikant beschränkt wurde. In einem solchen Falle führt ein (oftmals populistisch geprägter) Interessenwandel einer demokratischen Regierung dazu, dass diese ihre eigenen Interessen über die demokratische Verfasstheit der politischen Institutionen stellt und in der Folge die Interdependenzbeziehung zu den übrigen domestischen AkteurInnen stärker zu ihren Gunsten modifizieren kann.

Zusammenfassend zeichnen sich liberale Demokratien somit durch schwächere Interessensdurchsetzungschancen gegenüber domestischen AkteurInnen des gesellschaftlichen Spektrums aus. Anhand der gesellschaftlichen Präferenzen lässt sich dies jedoch damit erklären, dass für liberale Demokratien die eigenen Interessen stärker mit denen der breiten, an der Herrschaft zumindest partiell beteiligten Bevölkerung korrespondieren und die hierdurch eingeschränkte politische Autonomie zugunsten

41 In ihrem Buch »*Wie Demokratien sterben*« beschreiben Levitsky and Ziblatt 2018 verschiedene Mechanismen, die zur gewaltfreien Aushöhlung demokratischer Institutionen und Prinzipien seitens demokratischer EntscheiderInnen zur Anwendung gebracht werden können. Beispiele wären die politisch motivierte Besetzung bedeutsamer RichterInnenämter, oder auch die ideelle Untergrabung der Legitimität der traditionellen Medienlandschaft.

42 Diese sind: Bürgerliche Rechte, politische Freiheiten, horizontale Verantwortlichkeiten, effektive Regierungsgewalt sowie die zentrale Ebene des Wahlregimes.

der demokratischen und rechtsstaatlichen Integrität politischer Institutionen bewusst in Kauf genommen wird. In illiberalen Demokratien entwickeln politische EntscheiderInnen dagegen entsprechend dem ausgrenzenden Legitimationsansatz zunehmend Interessen, die den Interessen der breiten Bevölkerung entgegenstehen. Ein weiteres Charakteristikum illiberaler Demokratien kann zudem die zunehmende Erosion der Akzeptanz des Wahlergebnisses seitens der VerliererInnen sein, indem diese von Wahlbetrug und Fälschung sprechen und ihre AnhängerInnenschaft zu Protesten aufrufen. Der ›Sturm auf das Kapitol‹ in den USA am 6. Januar 2021 war hierfür ein prägnantes Beispiel (Shafy 2022).

Bei der Entstehung illiberaler Tendenzen in etablierten Demokratien können institutionelle Merkmale auf republikanischer Ebene eine besondere Rolle spielen. So geht der Liberalismus davon aus, dass Mehrheitsdemokratien grundlegend unkooperativere Strategien nach innen (und außen) verfolgen und in Folge wechselnder Mehrheiten gleichzeitig unzuverlässigere VerhandlungspartnerInnen auf domestischer (und externer) Ebene darstellen (Schimmelfennig 2013, S. 150). Durch das ›The-Winner-takes-it-all‹-Prinzip ist der Herrschaftszugang in solchen Systemen stärker auf die regierende Partei beschränkt, vor allem in Zweiparteiensystemen wie den USA (Meyer 2009, S. 96). Eine bereits im Wahlkampf stärker ausgeprägte Polarisierung zwischen den Lagern kann sich in der Folge vor allem dann auch auf republikanischer Ebene in illiberalen Tendenzen niederschlagen, sofern der/die KandidatIn einer populistischen Partei gewinnt. Populismus wird oftmals mit Ressentiments gegenüber bestehenden politischen Institutionen verbunden. Somit können populistische Regierungen speziell in Mehrheitsdemokratien diese in der Folge eines Wahlsieges effektiver schwächen und gleichzeitig deren liberalen Kern aushöhlen. Interessant ist hierbei jedoch, dass diese Einschränkung demokratischer Institutionen auf republikanischer Ebene von Populisten wie Donald Trump oftmals mit dem Argument vollzogen wird, dass hierdurch die Stimme des Volkes gegenüber dem Establishment durchgesetzt (Mudde 2004, S. 546), in liberaler Terminologie somit der Transmissionsriemen voll zur Entfaltung gebracht würde. Dies geschieht jedoch de facto durch die Schwächung demokratisch konstituierter Institutionen auf republikanischer und ideeller Ebene, wodurch es schlussendlich zu einer Kompromittierung des Transmissionsriemens und zu einer noch stärkeren Zentralisierung des Herrschaftszuganges unter der Ägide der Regierung und ihrer AnhängerInnen kommt. Im Gegensatz dazu sind Konsensdemokratien mit ihren korporatistischen Interessensgruppierungen stärker auf »*compromise and concertation*« (Lijphart 2012, S. 3) ausgerichtet. Die Macht ist bei diesen auf mehr politische AkteurInnen aus allen drei politischen Gewalten aufgeteilt. Zudem erfordert das Verhältniswahlsystem eine größere Kooperation zwischen den AkteurInnen eines Mehrparteiensystems, auch über die nächste Wahl hinaus. Die Durchsetzung populistischer Präferenzen und die Aufweichung demokratischer Institutionen sind in solchen Systemen somit aufgrund des dezentraleren Herrschaftszugangs politischer AkteurInnen schwerer durchzusetzen als in Mehrheitsdemokratien.[43]

43 Von diesem Grundsatz gibt es jedoch auch Abweichungen: So können auch bei Verhältniswahlen rechtspopulistische Parteien zusammen die Mehrheit gewinnen und in der Folge trotz der Notwendigkeit einer Koalitionsbildung ihre illiberalen Präferenzen sukzessive umsetzen, so gesche-

4.4.6 Die nationale Cyberakteursumwelt

Für die Operationalisierung der KV wird für beide Regimetypen ein Mix aus quantitativen und qualitativen Indikatoren herangezogen:

1. Staatliche/behördliche und privatwirtschaftliche Ebene

Der ›National Cyber Power Index‹ (NCPI) des Belfer Center aus Harvard sieht ein mehrdimensionales Bewertungsraster für staatliche Intentionen und staatliche Kapazitäten vor. Aus Sicht der offensiven Cyberproxynutzung werden für letztere primär die Aspekte ›Disabling Adversary Infrastructure (Offense)‹, ›Intelligence-Collection‹ und ›Commercial Gain‹ als relevant erachtet. Die teilweise überlappenden Teilindikatoren (linke Spalte, Tabelle 8) sowie deren Operationalisierungen (Ausprägungen in Tabelle 8) werden für die Bewertung der KV auf autokratischer Seite herangezogen, da diese hierdurch sowohl auf der staatlichen/behördlichen als auch auf der privatwirtschaftlichen Ebene möglich wird. Letztere ist besonders für IT-Unternehmen als demokratische Cyberproxys bedeutsam.

2. Die zivilgesellschaftliche Ebene: HacktivistInnen, UniversitätsabsolventInnen etc.

Auch zivilgesellschaftliche AkteurInnen können als Proxys fungieren. Darunter gefasst werden Personen mit entsprechenden technischen Fähigkeiten, die sie im Rahmen politischer, kommerzieller, akademischer oder krimineller Institutionen/Organisationen eingesetzt haben. Dies könnten HacktivistInnen, patriotische HackerInnen, aber auch UniversitätsabsolventInnen technischer Studiengänge der jeweiligen Länder sein. Im Rahmen der Analyse der KV wird somit an dieser Stelle (in Abwesenheit passender quantitativer Indizes über einen hinreichend großen Teil des Untersuchungszeitraumes) in erster Linie auf entsprechende Primär- und Sekundärquellen verwiesen, die die Existenz und das Ausmaß entsprechender AkteurInnen für die jeweilige Autokratie aufzeigen.

3. Die Ebene der Cyberkriminalität

Zuletzt stellt besonders der nationale Cyberkriminalitätssektor einen potenziellen Ressourcen-Pool für autokratische Cyberproxys dar. Dabei kann es sich um zunehmend im Cyberspace agierende Kriminelle handeln oder aber um genuine Cyberkriminelle, die ausschließlich im Cyberspace aktiv sind. Wie im Falle der zivilgesellschaftlichen Ebene wird zu deren Analyse auf Primär- und Sekundärquellen zurückgegriffen, die das Ausmaß und die Art der jeweiligen nationalen Cyberkriminalitätslandschaft erfassen.

Generell gilt, dass materielle sowie immaterielle Ressourcen vor allem staatlicher, aber auch nichtstaatlicher AkteurInnen aufgrund der im Vergleich zu konventionellen

---

hen etwa in Ungarn seit 2010 (Filippov 2021). In anderen europäischen Ländern, z.B. Deutschland, verhinderte dies bislang die Haltung etablierter konservativer Parteien, eine Regierungsbildung mit rechtsgesinnten Parteien wie der AfD von vornherein auszuschließen.

Machtdomänen wesentlich stärker auf Geheimhaltung basierenden Dynamik im Cyberspace weniger offensichtlich sind (Schulze 2019, S. 26). Daher ist für eine annähernde Bewertung der hier vorgeschlagene Mix aus quantitativen sowie qualitativen Quellen unterschiedlicher AkteurInnen erforderlich, wie er auch im Rahmen des NCPI zur Anwendung kommt (Voo et al. 2020).

Tabelle 8: Operationalisierung der KV

NCPI-Teilindikatoren* *(staatliche Ziele)*	Operationalisierung
Cyber-Military-Doctrine *(Offense)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Webseiten der jeweiligen Regierungen/Ministerien*)
Cyber-Military-Staffing/National Cyber-Command *(Offense)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Webseiten der jeweiligen Regierungen/Ministerien*)
Global Top-Technology-/Cybersecurity-Firms *(Offense, Commercial Gain, Intelligence)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Cybercrime Magazin, Forbes?*)
High-Tech-Exports *(Offense, Commercial Gain, Intelligence)*	Vorhanden? Wenn ja, seit wann? (*Quellen: World Bank*)

Die Tabelle basiert auf Voo et al. 2020.
* Der Teilindikator ›Existence of Private Sector Surveillance-Technology‹ wurde nicht noch einmal gesondert übernommen, da er deutliche Überschneidungen mit dem ebenfalls enthaltenen Indikator ›High-Tech-Exports‹ aufweist. Gleiches gilt für den Indikator ›Skilled Employees in the Technology-Industry‹ bezüglich des gelisteten Indikators ›Global Top-Technology-/Cybersecurity-Firms‹.

4.4.7 Das allgemeine Konfliktniveau

Für die Operationalisierung des intervenierenden Einflusses gewaltfreier und/oder gewaltsamer Konfliktdynamiken auf der konventionellen Ebene wird der bereits im HD-CY.CON angelegte Nexus zur konventionellen Konfliktforschung des HIIK genutzt. Wie bereits beschrieben, wird in Bezug auf Cybervorfälle nicht nur (sofern plausibel) der angenommene Cyberkonfliktgegenstand kodiert, sondern im Falle eines hiermit verbundenen konventionellen Konfliktes der betroffenen Dyade deren äquivalente Konfliktgegenstände. Darüber hinaus kann die Intensität des Cybervorfalls mit Werten von eins bis fünf zu dessen potenzieller HIIK-Konfliktintensität in Beziehung gesetzt werden.

Neben diesen quantitativen Indikatoren werden qualitative Quellen bezüglich der jeweiligen Konfliktdyaden analysiert, um den Einfluss der Konfliktereignisse auf der konventionellen Ebene im Sinne der aufgestellten Hypothesen testen zu können.[44]

4.5 Auswahl der Leitfragen

Die Auswahl der Leitfragen orientiert sich am liberalen Erklärungsmodell für die Verwendung von Proxys in Cyberkonflikten sowie der Struktur der ausgewählten Fälle. Aus den eingangs formulierten Gesamtforschungsfragen der Arbeit *(»Welche Arten von Proxys im Cyberspace nutzen Autokratien und Demokratien trotz eigener, technischer Kapazitäten? Welche Funktionen übernehmen diese und unter welchen Bedingungen?«)*, ergeben sich folgende, übergeordnete Leitfragen für beide Regimetypen, die die jeweiligen Fallstudien strukturieren:

- Welche Ausprägungen nehmen die beiden AVs in den jeweiligen Fällen an?
- Welchen Einfluss hatte die UV im Zusammenspiel mit den IVs und der KV auf die jeweilige(n) Ausprägung(en) der beiden AVs im betreffenden Fall und lassen sich hierüber Varianzen zwischen den Fällen erklären?
- Welche Befunde der Fallstudien konterkarieren die aufgestellten Hypothesen über die jeweiligen Wirkweisen der Variablen?

Für die Untersuchung autokratischer Cyberproxy-Nutzung bedeutet dies im Hinblick auf die beiden **AVs** folgende Untersuchungsfragen, die implizit beantwortet werden:

- Welche Funktion(en) im Sinne der prävalenten Incident-Types können für den jeweiligen Fall als vorherrschend bezeichnet werden? (AV I)
- Durch welche technischen und zielspezifischen Charakteristika zeichnete sich die Mehrheit der Angriffe aus?
- Welche Durchschnittsintensität bzw. Intensität in Abhängigkeit von der jeweiligen Incident-Type-Klasse liegt für den jeweiligen Fall vor? (AV I)
- Wie lassen sich die am häufigsten/stärksten genutzten Proxys für den jeweiligen Fall hinsichtlich ihrer Art und institutionellen Anbindung charakterisieren? (AV II)
- Lassen sich ›Within-Case‹-Varianzen feststellen? (AV I und AV II)

Für die demokratische Cyberproxy-Nutzung ergeben sich folgende Forschungsfragen zur Analyse der AVs:

- Welche Art von AkteurInnen attribuierte die Mehrzahl der jeweiligen Angriffe? Politische und/oder private AkteurInnen? (AV II)

44 Da das HIIK für manche Konfliktdyaden, wie etwa Iran vs. Saudi-Arabien im Jahr 2015, aus nicht ersichtlichen Gründen zeitweilig keine Kodierungen bereithält, müssen diese zusätzlichen Quellen analysiert werden.

- Welche Art von Zuschreibung wurde vorgenommen? (Blurred[45] vs. True Attribution?) (AV I)
- Wie gestaltete sich die zeitliche Abfolge der getätigten Attributionen (politische vs. technische) in den jeweiligen Fällen?
- Bezog sich die politische Zuschreibung (falls vorhanden) in irgendeiner Weise auf den IT-Sektor und seine Arbeit?
- Gibt es Hinweise oder Belege für eine tatsächliche Zusammenarbeit von Regierungsstellen sowie IT-Unternehmen im Vorfeld von Zuschreibungen?
- Sind personelle Verbindungen zwischen den attribuierenden IT-Firmen sowie der jeweiligen Regierung bekannt?

Um die Ausprägung sowie Wirkweise von UV, IV und KV im jeweiligen Fall bewerten zu können, werden für beide Regimetypen folgende Forschungsfragen implizit beantwortet:

UV:

- Welche domestischen AkteurInnen können für die jeweils zu erklärende Cyberproxy-Nutzung als besonders relevant erachtet werden? (Identifizierung der zentralen Winning Coalitions/Interessensgruppen mit Bezügen zur republikanischen Ebene)
- Wie waren deren Präferenzen auf ideeller und wirtschaftlicher Ebene ausgestaltet bzw. wie führte deren Ausgestaltung zur für die Proxy-Nutzung maßgeblichen Präferenzkonfliktivität gegenüber dem attribuierten Angreifer?
- Welchen Einfluss nahm die republikanische Ebene auf die Interessensdurchsetzung besagter AkteurInnen?
- Auf welche Weise konstituierte die republikanische Ebene selbst die für die Proxy-Nutzung maßgeblichen Vulnerabilitätsasymmetrien nach innen oder außen?

IV:

- Welchen Einfluss hatte das jeweilige allgemeine Konfliktniveau auf die Präferenzkonstellation auf domestischer Ebene?
- Inwiefern nahm das allgemeine Konfliktniveau somit einen direkten Einfluss auf die wahrgenommenen, eigenen oder fremden Vulnerabilitätsasymmetrien, die es durch die Proxy-Nutzung zu manipulieren galt?

KV:
Durch die Fallauswahl ergibt sich für die KV bereits notwendigerweise eine positive Ausprägung im Sinne des Vorhandenseins staatlicher sowie nichtstaatlicher AkteurInnen

45 Als ›Blurred Attributions‹ werden in der Folge solche Zuschreibungen bezeichnet, die keinen spezifischen Akteur als Verantwortlichen benannt haben und beispielsweise nur von ›TäterInnen aus dem Land X‹ oder ›vermutlich staatlich gesponserten AkteurInnen‹ ohne Nennung eines konkreten Landes sprechen.

mit entsprechenden Fähigkeiten im Cyberspace, weshalb im Rahmen der empirischen Untersuchung für deren Analyse folgende Frage im Mittelpunkt steht:

- Inwiefern konditionierte die KV durch ihre Ausprägung die jeweilige Cyberproxy-Nutzung autokratischer oder demokratischer Staaten, insbesondere im Hinblick auf die AV II?