6. Befunde und Implikationen

Insgesamt kann für beide Regimetypen konstatiert werden, dass diese aufgrund der aufgezeigten Funktionen ihre Proxys im Cyberspace entgegen der für traditionelle Proxys getätigten Beobachtung stärker als politisches Medium denn als militärisches ansehen (vgl. Moghadam und Wyss 2020, S. 121). Zweitens erscheinen nichtstaatliche AkteurInnen im Cyberspace immer nur so stark, wie es der jeweilige Staat zulässt. Dies gilt für Autokratien, zunehmend aber auch für Demokratien (Stichworte: ›Balkanisierung/Renationalisierung des Internets‹). Nachfolgend werden die zentralen Befunde für beide Regimetypen zusammengefasst und kritisch reflektiert.

6.1 Autokratien und ihre Cyberproxys

Für autokratische Regime und ihre Cyberproxys werden aufgrund der vergleichenden Fallstudien folgende Befunde nochmals betont und kritisch reflektiert:

Ohne völkerrechtlich verbindliche Regeln im Cyberspace, die besonders auch durch Normbildungsprozesse entstehen können, ist der autokratischen Nutzung von Cyberproxys kaum Einhalt zu gebieten. Öffentliche Attributionen demokratischer Länder, die jedoch nicht mit entsprechenden völkerrechtlichen Gegenmaßnahmen kombiniert wurden, entwickelten bislang keine entscheidende Abschreckungswirkung, da Autokratien darauf in erster Linie nicht durch eine funktionale, sondern personelle/organisatorische Umstrukturierung, auch mithilfe von Proxys, reagierten.

Die autokratischen Fallstudien zeigten ferner, dass es scheinbar zu einer Art Proliferation von Strategien, Techniken und Methoden im Cyberspace zwischen autokratischen Staaten kommen kann. Es kann dabei von einer inversen Logik zwischen China und Russland gesprochen werden: Während sich China im Bereich seines offensiven Cyberkonfliktaustrages teilweise inhaltlich durch stärker disruptive und militärisch integrierte Cyberattacken sowie operativ durch die vermehrte Integration unterschiedlicher Proxys wie Unternehmen oder wissenschaftlicher Einrichtungen dem russischen Modell anzupassen scheint, ist für Russland im Bereich der Internet-Governance eine zunehmende Annäherung an das chinesische System der ›Great Firewall of China‹ festzustellen. China übernimmt somit im Cyberkonfliktaustrag gegenüber der externen Umwelt

partiell russische Methoden und Strategien und Russland im Gegenzug chinesische im eigenen Umgang mit der nationalen Informationssouveränität, die nicht zuletzt auch der Abschottung nach außen dienen soll (vgl. Saalman 2017).

In der Analyse wurde zudem gezeigt, dass offensive Proxy-Nutzung tatsächlich auf die jeweilige Interessenlage der autokratischen Führung ausgerichtet ist: So lässt sich z.B. für Russland (zumindest vor dem Angriff auf die Ukraine im Februar 2022 und den daraus resultierten Wirtschaftssanktionen) kein weitflächiger, ökonomisch motivierter Datendiebstahl wie im Falle Chinas beobachten, obwohl dieselbe Praxis ja auch russischen Cyberproxys offen steht. Zentral sind demnach die eigenen Verwundbarkeitsasymmetrien. Dem bloßen Ausnutzen von Gelegenheiten ist geringere Bedeutung beizumessen. Ferner zeigt sich, dass sich Russland mit seinen disruptiveren Cyberoperationen stärker in direkte Opposition zur internationalen, liberal-demokratisch geprägten Staatenumwelt begeben hat, als China. Für die Interessensdurchsetzung der VR galt es auf außenpolitischer Ebene bislang IOs nicht öffentlich zu unterminieren, sondern stattdessen von innen heraus zum eigenen Vorteil zu nutzen, dasselbe gilt für wirtschaftliche Interdependenzverhältnisse mit demokratischen Staaten.

Für den Einfluss der KV auf die autokratische Cyberproxy-Nutzung konnte aufgezeigt werden, dass die Cyberkonflikt-Akteurslandschaft in beiden Fällen die Auswahl der Akteurstypen als Proxys grundlegend bestimmte. Bei Russland waren dies aufgrund des Zerfalls der UdSSR und vieler arbeitsloser InformatikerInnen eher AkteurInnen der Cyberkriminalitätsszene; bei China aufgrund des eingeschlagenen Modernisierungs- und Wirtschaftsentwicklungswegs vor allem auch Frontunternehmen des Technologiesektors. Für China deutet sich durch die zunehmend berichteten Moonlighting-Aktivitäten jedoch ein potenzieller Wandel zu stärkerer Cyberkriminalität von AkteurInnen an, die als staatliche Proxys begonnen haben.

Für Russland ist in der Retrospektive besonders seit Februar 2022 aufgrund des Angriffs auf die Ukraine für den Einfluss des allgemeinen Konfliktniveaus von Interesse, welche Rolle Cyberoperationen allgemein und Cyberproxys im Speziellen hierbei spiel(t)en.. Wirkliche ›Plausible Deniability‹ der vier genannten Hauptgruppierungen (Fancy Bear/APT28, Cozy Bear/APT29, Sandworm und Turla) scheint kaum noch zu existieren. Ist also beispielsweise nach wie vor Sandworm für die Sabotage kritischer Infrastrukturen verantwortlich, da primär nicht mehr die Verschleierung der Verantwortlichkeit im Vordergrund steht, sondern die (erfolgreiche) Durchführung der Operation an sich? Oder wurden neue AkteurInnen, z.B. Hacktivisten oder Cyberkriminelle gefunden, die wieder größere Ambivalenz bei der Attribution im Sinne ›echter‹ Cyberproxys garantieren? Auch die Reaktion westlicher Demokratien auf russische Cyberoperationen kann hierauf einen großen Einfluss nehmen.

Für China wird dagegen die Weiterentwicklung militärischer Konflikte im asiatischen Raum zeigen, inwiefern sich diese Konflikte verschärfen oder entspannen. Anzunehmen ist jedoch Folgendes: Je eskalativer diese konventionellen Konflikte werden, desto stärker wird die SSF eingesetzt, um Manöver durch Cyberoperationen zu ergänzen. Die berichtete Episode um den Stromausfall in Mumbai 2020 hat bereits angedeutet, dass auch China kritische Infrastrukturen militärischer Kontrahenten zunehmend ins Visier nehmen könnte.

Zuletzt deutete die Debatte um international anerkannte und erfolgreiche IT-Unternehmen als mögliche Cyberproxys autokratischer Staaten an, dass auch deren Verhältnis zum eigenen Staat nicht nur von Vorteilnahme geprägt ist: Die KPC reagierte auf aus ihrer Sicht potenziell regimegefährdende Aktivitäten ihrer großen Technologie-Unternehmen wie Alibaba von Jack Ma mit internen Repressionen und auch Russland verschärfte im Umgang mit dem bekannten IT-Unternehmen IB-Group 2021 die staatliche Kontrolle.

6.2 Demokratien und ihre Cyberproxys

Für demokratische Cyberproxys muss konstatiert werden, dass IT-Firmen eher punktuell als wirkliche Proxys im Sinne stellvertretender, durch den Staat beauftragte oder unterstützte Attributionen agieren. Es konnte keine verstetigte Staat-Proxy-Beziehung plausibilisiert werden, wie sie für zahlreiche offensive Proxys autokratischer Regime nachgewiesen werden konnte. Dabei verhinderten wohl auch erwartete wirtschaftliche Einbußen, wenn eine Firma zu sehr als verlängerter Arm der Regierung im Ausland gilt, eine stärkere Proxy-Funktionserfüllung. Verstärkt wird dies durch die steigende technologische Souveränität von Staaten mit wichtigen Absatzmärkten wie z.B. China.

Gleichzeitig verfügen private Unternehmen in Demokratien über eine größere Autonomie gegenüber ihren Regierungen als in den meisten Autokratien, da oftmals marktwirtschaftliche Strukturen dominieren und der Staat somit (zumindest relativ gesehen) weniger Einfluss- und Kontrollmöglichkeiten hat. ›Support‹ des Staates bezieht sich somit zumeist auf allgemeine Unterstützung der Unternehmen durch entsprechende (fehlende) Regulationen oder staatliche Aufträge und weniger auf konkrete Attributionsdirektiven. Der DNC-Hack/Leak demonstriert zudem, dass die Funktion der Schaffung von Legitimation einer erst verspätet erfolgenden politischen Attribution auch dahingehend kontestiert werden kann, falls ein Akteur des politischen Spektrums, in diesem Fall der gewählte Präsident, die Legitimation des (temporär) stellvertretend attribuierenden Unternehmens diskreditiert. IT-Unternehmen können in Demokratien Regierungen und deren Handlungen also nur Legitimation verleihen, sofern deren eigene Legitimation nicht durch Dritte angefochten wird. Die Episode zeigt zudem einmal mehr, dass Attribution schon lange keine rein rechtliche ›Ja/Nein‹-Frage mehr ist, sondern zahlreiche Grautöne, besonders durch Politisierung und Polarisierung, aufweist. Der Aspekt der ›richtigen‹ Vermittlung unterschiedlicher Attributionsevidenzen wird somit für liberale Demokratien immer entscheidender, sofern sie den Konflikt um die Deutungshoheit im Rahmen von Cyberkonflikten nicht an desinformationsorientierte Parteien verlieren wollen.

Obwohl für die USA und Israel defensive Cyberproxy-Funktionen plausibilisiert werden konnten, deutet deren Varianz hinsichtlich der Ausprägung der AV I auf die Relevanz demokratischer Subtypen hin. So wie die Regimetypen-Unterschiede zwischen Russland und China einen erheblichen Teil deren offensiver Cyberproxy-Nutzung erklären konnten (personalistisches vs. Einparteienregime), lassen sich auch die USA und Israel hinsichtlich der republikanischen Ausgestaltung des politischen Systems sowie ideeller und wirtschaftlicher Interessen nicht einfach miteinander vermengen. Vielmehr de-

monstrierten die vergleichenden Fallstudien, dass für die israelische Cyberproxy-Nutzung die Aufrechterhaltung historisch etablierter Taktiken wie der beschriebenen Ambivalenz im Umgang mit sicherheitspolitischen Gefahren eine umfassendere Rolle spielte als für die USA. Deren inhaltliche Cyberproxy-Nutzung hing dagegen stärker von den dominanten Interessensgruppierungen in Abhängigkeit von deren Verhältnis zum Präsidenten ab. Für Israel wird somit retrospektiv in der mittlerweile bereits wieder beendeten Post-Netanjahu-Ära von Interesse sein, inwiefern diese zeitweilige Varianz auf der republikanischen Ebene durch das (vorläufige) Ende der Likud-Ära auch eine Varianz in der Cyberproxy-Nutzung sowie der Cyberkonfliktstrategie im Allgemeinen bewirkt hat.

Sowohl für die USA als auch für Israel gilt es zudem, die seitens verschiedener BeobachterInnen hervorgehobene Nutzung privater AkteurInnen zu offensiven Zwecken im Cyberspace nicht aus den Augen zu verlieren, um das offensive Cyberproxy-Konzept nicht von vornherein auf Autokratien zu beschränken. Unabdingbar wäre hierfür jedoch eine weiterführende Differenzierung der unterschiedlichen Motivlagen, Staat-Proxy-Beziehungsmuster sowie rechtlichen Attribute zwischen autokratischen und demokratischen Cyberproxys im Offensivbereich, da hierbei – wie im Rahmen dieser Arbeit konstatiert – deutliche Unterschiede existieren.

Für Demokratien im Allgemeinen ist zudem die Etablierung von ›Plausible Deniability‹ im Cyberspace von Bedeutung: So könnte es entsprechend berichteter Beispiele aus dem konventionellen Bereich auch für Operationen im Cyberspace der Fall sein, dass sich demokratische Regierungen gegenüber geheimen Operationen ihrer SicherheitsakteurInnen in gewisser Weise absichern, um bei deren ungewollter Veröffentlichung eine Kenntnisnahme derselbigen ›plausibel bestreiten‹ zu können (vgl. Knott 2014). Da eine solche Praxis jedoch die Kontrolle der Politik über staatliche Behörden potenziell schwächen kann, gilt es, die Berichtspflichten demokratischer Cybereinheiten im Rahmen ihrer Offensivbefugnisse im Vergleich zwischen präsidentiellen und parlamentarischen Systemen kritisch auf den Prüfstand zu stellen.

6.3 Theoretische Implikationen

Der Liberalismus hat sich als tragfähiger theoretischer Ansatz erwiesen, um autokratische und demokratische Cyberproxy-Nutzungen zu analysieren. Bedeutsam ist sein Fokus auf nichtstaatliche AkteurInnen und deren Interessen: Nicht nur die reinen Machtasymmetrien entscheiden, wie vom Realismus vorhergesagt, über den Cyberkonfliktaustrag. Ansonsten dürfte es erstens neben den USA und vereinzelten weiteren Staaten keine im Cyberspace (erfolgreich) aktiven Staaten geben; zweitens dürften nichtstaatliche AkteurInnen dabei keine Rolle spielen; drittens dürfte es zwischen demokratischem und autokratischem Cyberkonfliktaustrag aufgrund der inneren Verfasstheit keine Unterschiede geben, zwei ähnlich ›mächtige‹ Demokratien und Autokratien müssten sich auch ähnlich verhalten; viertens müsste die Reaktion demokratischer Staaten auf autokratische Cyberangriffe ähnlich ausfallen wie die Reaktion auf Angriffe demokratischer Staaten, wenn deren Machtpotenziale als ähnlich gefährlich seitens der angegriffenen Demokratie eingeschätzt werden bzw. sonstige Interessenskonvergenzen keine Rolle spielen; und fünftens dürfte es zu keiner (*nicht*

hegemonial-indizierten) Kooperation im Cyberspace kommen. Stuxnet und weitere geheimdienstliche Kooperationen, etwa zwischen dem niederländischen Geheimdienst und dem FBI bei der Attribution von Cozy Bear 2016, beweisen jedoch das Gegenteil, da diese nicht als hegemonial indiziert betrachtet werden.

Dennoch zeigen der HD-CY.CON und dessen durchaus sozialkonstruktivistischer Ansatz gemäß dem Grundsatz »*Attribution is what states make of it*« (Rid und Buchanan 2015, S. 7), dass auch rationalistische Theorien wie der Liberalismus in Teilen durch sozialkonstruktivistische Elemente ergänzt werden könnten. So hat die Analyse auf Basis öffentlich zugänglicher Quellen und der darin berichteten Verantwortungszuweisungen entsprechend des liberalen Erklärungsansatzes plausibilisiert, inwiefern dieser die autokratische vs. demokratische Cyberproxy-Nutzung erklären kann. Wie vom Ansatz fokussiert, stellten die jeweiligen Präferenzordnungen der zentralen Interessensgruppen der Staaten die zentrale Erklärungsvariable dar, über die erklärt werden konnte, welche Asymmetrien mit welchen Proxy-Funktionen und durch welche Proxys verändert/manipuliert werden sollten. Die Dreiteilung in ideellen, kommerziellen und republikanischen Liberalismus ermöglichte es, den Einfluss der institutionellen Ausgestaltung des politischen Systems auf den Herrschaftszugang einzelner Gruppen zu identifizieren und in einem zweiten Schritt deren ideelle sowie kommerzielle Interessen zur staatlichen Cyberproxy-Nutzung in Beziehung zu setzen. Da sich die Analyse auf die im HD-CY.CON erfassten Kategorisierungen der einzelnen Gruppen und ihrer Angriffe als staatlich gesponsert bzw. allgemein/direktstaatlich stützte, ist dabei implizit die soziale Konstruktion der Attribution des Angreifers seitens der jeweiligen Attributionsquelle mit angelegt. Diesem Umstand wurde jedoch insofern Rechnung getragen, als im empirischen Teil entsprechend des Spektrums staatlicher Verantwortlichkeit untersucht wurde, inwiefern sich die jeweiligen Attributionen auf Basis öffentlicher Informationen stützen oder entkräften lassen. Dies verdeutlicht, dass auch das Cyberproxy-Konzept wie das Proxy-Konzept im Allgemeinen nicht frei von Deutungskonflikten ist.

Ferner entscheidet das normative Framing der eigenen Cyberproxy-Nutzung sowie der Fremdwahrnehmung besonders aufseiten befreundeter/alliierter Staaten über den öffentlichen Umgang hiermit, bzw., ob diese ebenso wie autokratische Cyberproxy-Spionage als unrechtmäßiges Verhalten angesehen bzw. öffentlich als solches deklariert wird. So waren und sind die USA offensichtlich davon überzeugt, dass ihre technologische Vormachtstellung dem Wohle der westlichen Staatenwelt dient und sie verpflichtet sind, alle möglichen Ressourcen zur Prävention oder Präemption potenziell staatsgefährdender Kräfte zu nutzen. Neben dem Liberalismus könnte also auch die sozialkonstruktivistische Rollentheorie ein geeigneter Ansatz zur Erfassung von Cyberproxys sein. Als Einschränkung wird hier jedoch eingewandt, dass das Proxy-Konzept stärker eine theoretische Meta-Rolle darstellt, die von außen AkteurInnen zugesprochen wird. Für eine rollentheoretische Analyse sollte die Proxy-Rolle somit mit weiteren, inhaltlichen Rollenkonzeptionen verbunden werden. Ansonsten ließen sich Bezüge zum Ego-Teil der jeweiligen Proxyrollenkonzeption wahrscheinlich weitaus schwerer herstellen als zum Alter-Teil.

In jedem Falle verschwimmt in der Empirie die Trennlinie zwischen tatsächlichen Proxys und direktstaatlichen Angriffen immer mehr, was gleichzeitig die beschriebenen theoretischen Herausforderungen und definitorischen Unterschiede in der Cyberproxy-

Konzeptualisierung erklärt. Angesichts der steigenden allgemeinen bzw. direktstaatlichen Attributionen demokratischer Staaten gegen autokratische CyberangreiferInnen stellt sich die Frage nach dem ›Verfallsdatum‹ des (offensiven) Cyberproxy-Konzepts. Wird die autokratische ›Plausible Deniability‹ immer unplausibler, könnten autokratische Regime wie Russland oder China, die auch auf staatlicher Ebene die notwendigen Fähigkeiten zur Durchführung von Cyberoperationen besitzen, in Zukunft auf Proxys ganz verzichten. An dieser Stelle gilt es jedoch zwischen der Proxy-Attribution und der tatsächlichen Einsetzung zu unterscheiden: Da neben der ›Plausible Deniability‹, wie aufgezeigt, auch interne Coup-Proofing-Erwägungen sowie fehlende Eigenkapazitäten auf autokratischer Seite zur Einsetzung von Proxys führen können, hätte eine gewandelte demokratische Attributionspraxis auf diese beiden stärker domestisch geprägten Motivlagen deutlich weniger Einfluss. In jedem Falle wird die Frage der rechtlichen Verantwortung der Staaten immer stärker Gegenstand politischer und daher notwendigerweise auch wissenschaftlicher Debatten.[1]

Es könnte somit in Zukunft zu einer Art Normalisierung offener direktstaatlicher Cyberangriffe kommen, wobei interessant sein wird, speziell die israelische Kommunikationsstrategie bezüglich eigener Operationen im Wandel der Zeit zu betrachten. Jedoch bleibt hierbei abzuwarten, inwieweit die Intensitätsschwelle, die das jeweilige Opfer zu einer physischen Reaktion zwingen würde, dabei regelmäßig und in welcher Form überschritten wird. Aus theoretischer Sicht stellt sich somit folgende Frage: Treibt die tatsächliche Staatenpraxis die internationale Normgenese vor sich her oder umgekehrt?

Ein weiterer theoretisch-analytischer Mehrwert der Arbeit betrifft den Umgang mit dem Proxy-Konzept an sich: Indem Proxys zum einen im Rahmen von Cyberoperationen untersucht wurden, dabei jedoch (auch) deren Beziehungen zum jeweiligen staatlichen Sponsor im Mittelpunkt standen sowie ferner Bezüge zu damit assoziierten konventionellen Konflikten hergestellt wurden, wurden in der Arbeit die beiden in der Proxy-Forschung bislang dominierenden Ansätze verbunden: der akteurszentrierte vs. der konfliktdomänenzentrierte Ansatz (Moghadam und Wyss 2020, S. 124). Hierdurch wird deutlich, dass nichtstaatliche AkteurInnen als Proxys im Cyberspace dienen können, dies jedoch zeitlich begrenzt sowie auf verschiedene Konfliktsphären bezogen sein kann. Cyberproxys stellen eben zumeist *nicht* das alleinige Konfliktmittel autokratischer und demokratischer Staaten dar, sondern eines unter mehreren. Die Übertragung des bislang rein offensiv verwendeten Cyberproxy-Konzepts auf demokratische Attributionspraktiken soll aufzeigen, welchen Nutzen das Proxy-Konzept zur theoriegeleiteten Erfassung demokratischer Verschleierungs- und Geheimhaltungstaktiken im Rahmen von Cyberkonflikten haben kann. Dennoch sollte bei einer solchen Modifikation eines bestehenden Konzepts stets die Gefahr eines »*concept stretching*« (Sartori 1970, S. 1034) berücksichtigt werden: Das Ziel sollte nicht sein, möglichst viel Empirie durch dasselbe Theoriekonzept erfassen zu können, sondern durch die Rekontextualisierung des Konzepts dessen Anknüpfungsfähigkeit auch an neuere Untersuchungsfelder zu überprüfen und ggf. auch

1 So beschäftigte sich im Jahr 2022 die ›Closing the Gap‹-Konferenzreihe des ›The Hague Program on International Cyber Security‹, gemeinsam u.a. mit der Initiative ›EU Cyber Direct‹, mit dem Thema der »*Responsibility in Cyberspace*« (s. The Hague Program on International Cyber Security 2022).

kritisch zu hinterfragen. Im Falle der hier konzeptualisierten demokratischen Cyberproxy-Nutzung ist sicherlich am stärksten der Delegations-/Unterstützungsmodus seitens Demokratien an IT-Unternehmen im Rahmen des Attributionsprozesses zu diskutieren. Es stellt sich konkret die Frage, wie direkt und fallspezifisch dieser (nachweisbar) sein sollte, um das Proxykonzept zur Anwendung bringen zu können.

Die empirischen Befunde zur Untersuchung russisch- und chinesischsprachiger Quellen legen ferner nahe, dass die Cyberkonfliktforschung ihren westlichen Bias auch nicht durch die Inklusion einzelner nichtwestlicher Quellen verliert. Erstens ist an diese nach wie vor schwerer heranzukommen, zweitens weisen diese ebenfalls Verzerrungen auf und drittens dominieren die westliche Sicht und die englische Sprache den Diskurs in der Threat Intelligence Community, insbesondere durch eine nach wie vor auf vielen Ebenen bestehende US-Dominanz. So sind die meisten verwendeten Komponenten der globalen IT-Infrastruktur wie Kabel, Software-Produkte, Hardware-Produkte, Social-Media-Plattformen etc. US-Produkte, wodurch sich auch der Streit um die Involvierung Huaweis am Aufbau der 5-G-Netze erklärt.

6.4 Anknüpfungspunkte für künftige Forschungsvorhaben

Aus den diskutierten empirischen Befunden und theoretischen Überlegungen ergeben sich zahlreiche Anknüpfungspunkte für künftige Forschungsvorhaben im hier bearbeiteten Themenfeld.

Beginnend mit der VR China als Untersuchungsfall, könnten weitere Studien analysieren, inwiefern Xis personalisierter Machtzugang in Zukunft stärker durch KPC-Eliten kontestiert wird und welchen Einfluss dies auf den offensiven Cyberkonfliktaustrag des Landes hat. Zudem stellt sich die Frage, wie die PLA im Falle einer Eskalation im Südchinesischen Meer oder gegen Taiwan im Cyberspace performieren würde. Konkret könnte dabei die Rolle von Cyberoperationen auf strategischer, operativer und taktischer Ebene untersucht werden.

Daran anknüpfend könnte jedoch auch die Rolle der PLA auf domestischer Ebene Gegenstand weiterer Arbeiten sein, etwa um herauszufinden, ob sie auch disruptiv gegen nationale Ziele vorgeht und, falls ja, in welchem Zusammenhang dies mit gewaltsamen Repressalien gegen die betroffenen AkteurInnen steht.

Für das MSS wird die Zukunft zeigen müssen, ob es an der in dieser Arbeit aufgezeigten Nutzung kommerzieller Proxys auch in Zukunft festhält. Künftige Arbeiten könnten somit den Einfluss der KV über die Zeit in den Blick nehmen: Ist in Zukunft für China eine noch stärkere Nutzung von Moonlightern bzw. Cyberkriminellen zu erwarten? Falls ja, welchen Einfluss nahmen demokratische Sanktionen (auch im Rahmen der Cyber Diplomacy Toolbox der EU) gegenüber den bislang als Proxys präferierten Frontunternehmen hierauf? Schiebt das MSS in Zukunft den kriminellen Aktivitäten der Moonlighter einen Riegel vor aufgrund steigenden internationalen Drucks und im Vergleich zu Russland salienterer, wirtschaftlicher Interdependenzbeziehungen zu demokratischen Staaten? Welche Rolle könnte dabei analog zur russischen ›Ransomware Diplomacy‹ in der Ukraine-Krise eine mögliche Zuspitzung des Konflikts um Taiwan spielen und den chi-

nesischen Umgang mit nationalen HackerInnen als Verhandlungsmittel gegenüber dem Westen?

Auch für Chinas Verhalten auf internationaler Ebene ergeben sich weiterführende Fragen: Wird die VR auch im Rahmen internationaler Verhandlungen über die Verregelung des Cyberspace eine noch proaktivere Rolle einnehmen, ähnlich wie Russland im Bereich der Cyberkriminalität? Falls ja, inwiefern sind die dabei artikulierten Interessen/Forderungen am eigenen Cyberkonfliktaustrag ausgerichtet bzw. inwiefern soll dieser hierdurch geschützt bzw. ermöglicht werden?

Für Russland bleibt auch nach dieser Arbeit weitgehend unklar, inwiefern Proxys oder Hacker unterschiedlicher Geheimdienste die Operationen der anderen versuchen zu kompromittieren, um deren Interessensdurchsetzungschancen zu schwächen oder einzuhegen. Indizien für ein solches Verhalten gibt es auf der konventionellen Ebene bereits. Die noch tiefergehende Analyse des Verhältnisses der verschiedenen russischen Cyberoperationen im Hinblick auf die grundlegende und jeweils temporäre Beziehung der im Hintergrund verantwortlichen Teile der Winning Coalition zueinander könnte somit einen weiteren Beitrag der Forschung zum russischen Cyberkonfliktaustrag darstellen und auf den Erkenntnissen dieser Fallstudie aufbauen. Dies gilt insbesondere für den Zeitraum während (und potenziell nach) dem Krieg gegen die Ukraine ab Februar 2022, der zu Verschiebungen innerhalb des russischen Machtgefüges auf der konventionellen sowie der Cyber-Ebene führen dürfte.

Weitere Arbeiten könnten für Russland zudem das Verhältnis von Ransomware-Gruppierungen zu staatlichen Stellen sowie deren Integration in die russische Kriegsstrategie in der Ukraine in den Blick nehmen. Die sogenannten »Conti-Leaks« haben gezeigt, dass ursprünglich ökonomisch motivierte Akteure im Kontext geopolitischer Konflikte ihre Präferenzordnung zu Gunsten ideell-nationaler Interessen verändern können und somit nicht mehr als Cyberproxys agieren wollen.[2] Interne Interessenskonflikte können somit die Nützlichkeit einzelner Proxygruppierungen über Zeit schwächen und alternative Rekrutierungsaktionen, wie etwa die Mobilisierung von Gefängnisinsassen mit IT-Kenntnissen in Russland erforderlich machen (Krebs 2022). Nichtsdestotrotz kann Ransomware für Russland (wie bereits zuvor für Nordkorea) ein Baustein sein, um zumindest zeitweise den Druck internationaler Sanktionen abzumildern und so die eigene, Output-orientierte Regimesicherheit durch die erbeuteten Gewinne zu stärken.

Für die Zeit nach Putin wird von besonderem Interesse sein, inwiefern dessen Nachfolger gleichsam im Stande sein wird, das Konkurrenzstreben der Geheimdienste in weitgehend geordneten Bahnen zu halten, oder ob sich einzelne Teile daraus zu einer ernsthafteren Bedrohung für den Kreml entwickeln, als es unter der personalisierten und zentralisierten Führung Putins bislang der Fall war. Die Interessensdurchsetzung der verschiedenen Geheimdienste unter Putin scheint dagegen weniger von deren Bedrohungspotenzial als ihrer faktischen Performanz zur Regimesicherung abhängig zu sein. Ein Machtverlust der Kreml-Spitze nach Putin gegenüber Teilen der Winning

2 Ein mutmaßlich ukrainisches Mitglied der Ransomware-Gang Conti hatte nach deren öffentlicher Loyalitätsbekundung zu Russland interne Daten und Informationen u.a. auch Source-Code der Gruppe öffentlich gemacht (Knop 2022).

Coalition könnte auch einen Einfluss auf das hier analysierte russische Cyberkonfliktverhalten haben, zu größeren Kollateralschäden, noch häufiger sich konterkarierenden Paralleloperationen sowie noch stärkeren geopolitischen Verwerfungen führen. Ein ›Post-Putin‹-Russland könnte jedoch auch stärker demokratische Züge annehmen, je nachdem, wie stark der Modus des Machtübergangs seitens des Regimes gesteuert wird. Käme es aufgrund von zunehmenden domestischen Protesten, etwa aufgrund des (Ausgangs des) Kriegs gegen die Ukraine zu Wahlen, in denen liberale Oppositionsparteien eine tatsächliche Chance auf die Mehrheit hätten, könnte sich auch der russische Cyberkonfliktaustrag in Zukunft ›liberalisieren‹, demnach weniger die Unterwanderung liberal-demokratischer Länder sowie Institutionen zum Ziel haben. Ein solches Szenario erscheint zum aktuellen Zeitpunkt jedoch unwahrscheinlich.

China und Russland sind jedoch nicht die einzigen untersuchungswürdigen Autokratien im Cyberspace. Neben dem Iran und Nordkorea verweisen IT-Unternehmen auch immer wieder auf Vietnam und dessen Cybergruppierungen. Das US-Unternehmen Meta (vormals Facebook) veröffentlichte Ende 2020 einen Bericht, in dem Cyberoperationen mit vietnamesischen Technologie-Unternehmen in Verbindung gebracht wurden (Gleicher 2020). Somit könnte eine potenziell autokratische Cyberproxy-Strategie-Diffusion in den Blick genommen werden bzw. untersucht werden, ob es so etwas wie autokratische Staat-Proxy-Beziehungszyklen gibt, anhand derer prognostiziert werden kann, zu welchem Zeitpunkt ein Land primär auf welche nichtstaatlichen AkteurInnen als Cyberproxys zurückgreifen wird. Regionale Gemeinsamkeiten sowie Subtypenkategorisierungen könnten hierfür theoretische Ansatzpunkte sein.

Da in der vorliegenden Arbeit die Kategorisierungen ›Free‹ vs. ›Not Free‹ von Freedom House verwendet wurden, um möglichst große Regimetypenunterschiede zwischen den Fällen zu gewährleisten, wären für die Zukunft Studien zu hybriden oder im Transformationsprozess befindlichen Staaten wichtig (›Partly Free‹). Da im HD-CY.CON nur neun Proxy- und zehn allgemeine/direktstaatliche Operationen diesen Regimen als AngreiferInnen zugesprochen wurden, deutet sich bei diesen ein im Vergleich zu Autokratien und Demokratien deutlich niedrigeres Cyberoperationsengagement an. Künftige Forschungen könnten sich somit speziell mit diesen Regimen befassen und untersuchen, wie sich deren Cyberoperationsverhalten bei einer autokratischen oder demokratischen Transition verändert. Als theoretischer Anknüpfungspunkt könnte hier die Debatte um unterschiedlich hohe ›Eintrittsschwellen‹ in den staatlichen Cyberkonfliktaustrag dienen, die Max Smeets in seinem 2022 veröffentlichten Buch diskutiert.

Wie bereits angesprochen, stellt sich für Demokratien auch in Zukunft die Frage, ob im Cyberspace die tatsächliche Staatenpraxis die Normentwicklung vor sich hertreibt oder umgekehrt. In diesem Zusammenhang könnte der Einfluss unilateral gesetzter Cybersicherheitsstrategien (z.B. von Großbritannien Ende 2021) auf den demokratischen Normdiskurs und die Normgenese der internationalen Ebene untersuchungswürdig sein. Unmittelbar hiermit verbunden ist die nach wie vor nicht ausreichend behandelte Frage nach der Effektivität bisheriger und künftiger demokratischer Reaktionsoptionen auf autokratische Cyberoperationen. Konkret betrifft dies die EU Cyber Diplomacy Toolbox, die der EU mehr Schlagkraft bei der Bekämpfung und Abschreckung künftiger Angriffe verleihen soll. Daher sollte die bislang noch mehr auf den Aspekt der Attri-

bution ausgerichtete wissenschaftliche Debatte hieran noch stärker anknüpfen bzw. nachgelagerte Aspekte der Verantwortungszuweisung deutlicher berücksichtigen.

Für die USA wird ähnlich wie bei Regierungswechseln in Russland, China sowie Israel von Interesse sein, welchen Einfluss eine mögliche Wiederwahl Donald Trumps (oder ein republikanischer Sieg im Allgemeinen) 2024 auf die künftige Cyberpolitik des Landes haben könnte. Entscheidend könnte sein, auf welchem Stand die internationale Normgenese zu dieser Zeit wäre und ob sie sich entsprechend robust genug gegenüber potenziellen Unilateralismus- und Protektionismusbestrebungen einer republikanischen US-Regierung zeigen würde.

Für Israel als besonders stark von den eigenen Technologieexporten abhängige Demokratie wird sich infolge der Pegasus-Enthüllungen 2021 zeigen, ob und wie sich der Druck anderer Demokratien auf deren Geschäftsbeziehungen zu autokratischen Staaten auswirkt. Kommt es zu einer kontinuierlichen Präferenz für liberal-demokratische Grundwerte vor kommerziellen Interessen? Welchen Einfluss nimmt dies auf die Beziehung zwischen dem öffentlichen und privaten Sektor und die hier konzeptualisierte demokratische Cyberproxy-Nutzung? Auch hieran könnten künftige Forschungsarbeiten anknüpfen.

Ein letzter Aspekt betrifft die in der Arbeit angestrebte Methode unterstützender ExpertInneninterviews: Trotz zahlreicher und wiederholter Kontaktaufnahmen zu unterschiedlichen Akteursgruppierungen in unterschiedlichen Ländern über bereits bestehende Kontakte sowie offizielle Kanäle waren nur in wenigen Fällen Personen zu Interviews bereit. Dies betraf besonders politische/staatliche Institutionen in Deutschland. MitarbeiterInnen der Behörden meldeten konkret zurück, dass sie entweder generell keine Aussagen zu dieser Thematik äußern dürfen oder in Deutschland das Bundesamt für Verfassungsschutz (BfV) für öffentliche Attributionen zuständig sei. Das BfV erlaubt jedoch nur Interviews mit dem Präsidenten, was im Rahmen dieser Arbeit auch keine realistische Option war. Die Interviews mit den wissenschaftlichen Mitgliedern der US Cyber Solarium Comission deuten eine größere Offenheit der USA zu dieser Thematik an, gleichzeitig handelte es sich bei Brandon Valeriano und Erica Borghard auch um keine politischen EntscheidungsträgerInnen oder offizielle US-BeamtInnen. Eine transparentere Cybersicherheitspolitik demokratischer Staaten könnte für die Zukunft dieses offensichtlich zumindest in Teilen bestehende Vertraulichkeitsproblem gegenüber der Wissenschaft etwas aufbrechen, was den Raum für mehr solcher Interviews öffnen würde, die sich explizit mit öffentlicher vs. technischer Attribution von Cyberoperationen befassen.

6.5 Policy-Implikationen

Die Festlegung und öffentliche Kommunikation gewisser roter Linien erscheint auch für den staatlichen Cyberkonfliktaustrag auf internationaler Ebene unabdingbar. Dies sollte jedoch idealerweise nicht durch das Setzen unilateraler Grundsätze erfolgen, indem jeder Staat für sich selbst im Rahmen seiner nationalen Cybersicherheitsstrategie definiert, in welchen Fällen welche Formen offensiver oder reaktiver Cyberoperationen angewandt werden. Vielmehr sollte der bereits in zahlreichen Foren eingeschlagene Mul-

tistakeholder-Ansatz noch intensiviert werden, wobei jedoch eine effektivere Übertragung der dabei erzielten Ergebnisse auf letztlich ›verbindliche‹ Governance-Formate wie die UN notwendig wäre. Den hierfür notwendigen politischen Konsens herzustellen, ist alles andere als leicht. Begonnen werden sollte aus demokratischer Sicht mit den noch unentschlossenen demokratischen oder zumindest hybriden ›Swing States‹: Diese weisen grundlegende Interessenskonvergenzen mit demokratischen Ländern auch bezüglich des Cyberspace auf, tendieren in konkreten Fragen der Internet-Governance jedoch auch zu autokratischeren Modellen. In Joseph Nyes Worten müssten insgesamt demokratische Soft-Power-Potenziale somit autokratische Hard-Power-Potenziale als Anreizstruktur auch für diese Staaten überwiegen, damit sie sich in Grundsatzfragen auf die Seite des liberal-demokratischen Lagers stellen. Policy-Optionen hierfür wären z.B. substanzielle Unterstützungsleistungen bereits stärker entwickelter Staaten für den Aufbau nationaler Kapazitäten im Technologie-Bereich sowie ›Confidence-Building-Measures‹. Diese Unterstützungsleistungen sollten jedoch an demokratische Bedingungen geknüpft werden, damit die zu entwickelnden Fähigkeiten auch entsprechend eingesetzt werden. Grundvoraussetzung hierfür ist jedoch auch innerhalb der als liberale Demokratien bezeichneten Staatengemeinschaft ein Konsens über die hiermit angestrebten Ziele.

Gleichzeitig darf durch ein Kommunizieren roter Linien autokratischen AngreiferInnen nicht zu leicht signalisiert werden, dass alles unterhalb dieser Schwelle stillschweigend geduldet wird, denn sonst könnte dies konsequent und überbordend ausgenutzt werden. Zwei Wege wären hierfür denkbar: Der erste Weg würde über eine gesteigerte und effektivere Sanktionierung der jeweils als Täter identifizierten Autokratien führen. Hierfür müssten jedoch die den Sanktionen zu Grunde liegenden Attributionen auf breiten Konsens innerhalb der einzelnen Staaten sowie untereinander stoßen, da für deren Effektivität eine breite Anwendung seitens möglichst vieler Staaten notwendig ist. Diese Entscheidungen sollen durch ideelle Überzeugungsarbeit und weniger über das Androhen zwischendemokratischer Sanktionierungen wie das Aufkündigen des gegenseitigen Austauschs geheimdienstlicher Informationen erfolgen. Hierfür wäre jedoch das Erreichen des ›Tipping-Points‹ im ›Norm-Life-Cycle‹ erforderlich, damit es zu solch einer Norminternalisierung kommen kann (vgl. Finnemore und Sikkink 1998). Der zweite Weg sähe vor, dass im Zuge komplexen Lernens entsprechende Normbildungsprozesse entstehen. Dies könnte auf internationaler Ebene durch Issue-Linkage ermöglicht werden. Es stellt sich hierbei die Frage nach dem kollektiv besten Ergebnis und wie dieses durch gegenseitige Zugeständnisse über verschiedene Politikfelder hinweg erreicht werden kann. Wenn beispielsweise Autokratien im Rahmen der UN hinsichtlich eines angestrebten Cyberwaffenvertrages entgegengekommen wird, könnten diese als Gegenleistung verbindlich zusichern, keine Angriffe mehr auf demokratische Wahlen und deren IT-Infrastruktur durchzuführen. Bevor es hier jedoch zu einer wirklichen Norminternalisierung auf autokratischer Seite kommen könnte, würde insbesondere Verifikations- und Sanktionsmechanismen zur Überprüfung der ›Compliance‹ dieses Austauschs an angestrebten Gütern auf internationaler Ebene eine wichtige Bedeutung zukommen. Bereits für diese Verifikationsregime ist jedoch ein hinreichendes Maß an zwischenstaatlicher Kooperation notwendig, gerade in einem von Geheimhaltung geprägten Konfliktmedium wie dem Cyberspace. Daher würde

etwa eine internationale Cyberkonflikt-Attributionsagentur, ähnlich der Internationalen Atomenergie-Organisation (IAEA), noch größeren Herausforderungen in ihrer täglichen Arbeit gegenüberstehen als Regime des konventionellen Bereichs. Bereits für die Etablierung solcher Verifikationsregime, die letztlich Norminternalisierung erst ermöglichen sollen, ist somit ein Grundkonsens bezüglich der dem Regime zugrunde liegenden Normen notwendig (vgl. Haas 1980, S. 358).

Wie sich im Zuge des russischen Krieges gegen die Ukraine ab Februar 2022 zeigte, gilt es aus demokratischer Sicht zudem, die autokratischen Handlungen im Cyberspace im Rahmen gewaltsamer Konflikte nicht zu über- oder unterschätzen (vgl. Lonergan und Lonergan 2022). So sollten Cyberoperationen weder als deterministische Ankündigung nachfolgender Militärhandlungen gewertet noch ignoriert werden. Der Ansatz der USA unter Biden, die Ukraine durch die Entsendung von IT-ExpertInnen direkt bei der Prävention und Abwehr russischer Cyberoperationen zu unterstützen (Cooper und Barnes 2021), erscheint dabei sinnvoll, trägt er doch zu keiner direkten Eskalation des Konfliktes bei und stärkt gleichzeitig die ukrainische Cyberdefensive. Generell kann festgestellt werden, dass im Cyberspace ein defensiver »*deterrence by denial*« -Ansatz weitaus erfolgsversprechender erscheint, als der oftmals propagierte »*deterrence by punishment*«-Ansatz der Offensive (vgl. Nye 2017). Verstärktes Engagement zur Stärkung der Cyberdefensive nationaler sowie internationaler IT-Infrastrukturen, auf staatlicher und privater Ebene, sollte somit das oberste Ziel aller Regierungen sein. Gleichzeitig sollten besonders auf transatlantischer Seite Vorbereitungen für den Fall getroffen werden, dass Russland wie 2015/2016 doch noch (physisch) disruptive Cybersabotageoperationen gegen kritische Infrastrukturen der Ukraine, jedoch auch unterstützender Staaten, durchführen sollte. Um die Ukraine nicht noch stärker zum russischen ›Testbattlefield‹ im Cyberspace werden zu lassen, sollten daher klare Reaktionsoptionen für unterschiedliche russische Cyberoperationen abgesprochen und dann auch angewandt werden. Wie die US-Unterstützung der Ukraine entspräche dies der Umsetzung des UNGGE-Reports aus 2015, der die Gefahren von Cyberoperationen gegen kritische Infrastrukturen als einen Schwerpunkt hatte. Dieselbe Logik gilt auch für Taiwan und andere Länder im Südchinesischen Meer, sollten sich chinesische Cyberoperationen im Rahmen militärischer Auseinandersetzungen in Zukunft intensivieren. Insbesondere die Rolle offensiver Cyberproxys als AngreiferInnen sollte hierbei klar als unzureichend definiert werden, um den jeweils auftraggebenden Staat von einer auch rechtlichen Verantwortung freizusprechen. Individuelle Anklageerhebungen, zudem ohne strafrechtliche Effektivität, erscheinen hier bislang als unzureichende Mittel. Notwendig wären somit umfassende und glaubwürdige Attributionspraktiken auf Grundlage völkerrechtlicher Prinzipien, um sich nicht dem Vorwurf rein politisch motivierter Anschuldigungen auszusetzen. Dieser Punkt schließt an die noch stärker zu vereinheitlichende Attributionspraxis demokratischer Staaten gegenüber autokratischen CyberangreiferInnen an, was bereits bei den sich teilweise widersprechenden Namensgebungen von APTs beginnt. Dass dies in Zukunft auch einen Einfluss auf Schadensersatzforderungen im Rahmen abgeschlossener Versicherungen haben könnte, zeigen die Ausführungen der britischen ›Lloyd's Market Association‹ vom November 2021: Darin werden Cyberoperationen mit staatlicher Urheberschaft als Ausnahmen definiert, in welchen der Versicherungsschutz nicht greifen würde. Als zentraler Indikator hierfür wird die politische Attribution der Regierung des Landes benannt,

indem sich die betroffenen Computersysteme befinden. Findet eine solche politische Attribution jedoch nicht oder nur verzögert statt, könne der Versicherer eine Attribution in Richtung staatlicher AkteurInnen auch selbst vornehmen (Lloyd's Market Association 2021). Somit könnten hier neben privaten IT-Unternehmen weitere nichtstaatliche AkteurInnen künftig Cyberattributionen vornehmen, bislang noch nicht hinreichend definierte Standards weiter aufweichen und zudem aus kommerziellem Interesse auch Attributionsdruck auf nationale Regierungen ausüben.

Ferner sollten verschiedene Attributionsformen auch an unterschiedliche Reaktionsoptionen gekoppelt werden, um hier eine bessere Verhaltenserwartbarkeit zu schaffen (z.B. im Rahmen der EU Cyber Diplomacy Toolbox). Dies sollte aber auch hinreichend flexibel gehandhabt werden, um (wie zuvor angedeutet) zu verhindern, dass eine Autokratie das Verbleiben unter einer als besonders kritisch angesehen Intensitätsschwelle konsequent perfektioniert, die eigenen Operationen immer mehr ausweitet und so zu einer Normalisierung dieser Cyberoperationen beiträgt. Auch für einen solchen Fall sollten im Sinne einer kumulativen Intensitätsbewertung verhältnismäßige Reaktionsoptionen entwickelt werden.

Innerhalb der EU wird seit mehreren Jahren verstärkt das Konzept der ›technologischen/digitalen Souveränität‹ diskutiert, um weniger abhängig von den USA und Asien sowohl im Rahmen internationaler Lieferketten als auch bezüglich des Austausches geheimdienstlicher Informationen im transatlantischen Verhältnis zu werden. Letzteres erschien insbesondere aufgrund der Präsidentschaft Donald Trumps notwendig, der zuvor etablierte Prinzipien der Zusammenarbeit negierte und verstärkte Unsicherheit aufseiten der EuropäerInnen hervorrief. Sowohl aus wirtschaftlicher als auch sicherheitspolitischer Sicht könnte eine verstärkte Autonomie der EU somit positive Effekte haben, etwa indem der Zugang der USA zu Geheimdienstinformationen aus dem EU-Raum an Bedingungen geknüpft würde. Damit sich die EU diese Forderungen jedoch überhaupt leisten kann, wäre der Ausbau eigener geheimdienstlicher Kapazitäten erforderlich. Inwiefern dies bedeuten würde, dass die Geheimdienste der EU-Mitgliedstaaten hierzu vermehrt in fremde Netzwerke eindringen müssten, Sicherheitslücken ausnutzen und somit potenziell auch ungewollte Eskalationsspiralen in Gang setzen könnten, gelte es dabei jedoch zu bedenken. Gestärkt werden könnten hierdurch jedoch auch die europäischen Attributionskapazitäten, um die Anwendung der Cyber Diplomacy Toolbox auf von den USA unabhängigere Füße zu stellen.

Auch auf der noch technischeren Ebene ergeben sich aus den empirischen Ausführungen der Arbeit weitere Policy-Implikationen: Eine internationale Malware-Plattform, in die Länderbehörden Informationen über Vorfälle einspeisen und auf die auch (vorher zertifizierte und regelmäßig überprüfte) private IT-Unternehmen Zugriff haben, könnte dabei helfen, eine ›Cyberpandemie‹ wie NotPetya oder WannaCry in Zukunft zu verhindern bzw. zumindest schneller einzudämmen. Es müsste sich somit um eine Art Frühwarnsystem handeln, das jedoch effektiver funktioniert als bislang bereits bestehende Versuche in diesem Bereich. Es existieren jedoch auch Vorbehalte gegenüber dem Austausch von Malware-Samples z.B. auf VirusTotal, da dies bereits jetzt laut IT-ExpertInnen diverse Risiken für »Intrusion-Detection«- und »-Prevention«-Vorgänge sowie für die betroffenen AkteurInnen birgt. Denn durch das Hochladen der Malware-Samples können Personen mit Zugriffsrechten hierauf potenziell erkennen,

wer von dieser Malware betroffen war, wie der Exploit funktioniert und ggf. auch Einsicht in sensitive Informationen nehmen, falls diese Teil des Samples waren (vgl. Steffens 2020, S. 58). Es käme hier somit auf ein hinreichend vertrauensvolles Netzwerk an zertifizierten AkteurInnen an und zudem auf eine kontrollierte, standardisierte Form der Malware-Veröffentlichung, die den betroffenen AkteurInnen nicht zum Nachteil gereicht. Die Einbindung von Unternehmen in autokratischen Ländern impliziert stets die Gefahr der Weitergabe der technischen Informationen an staatliche Stellen. Wenn jedoch die zunehmende Fragmentierung des Internets aus demokratischer Sicht verhindert werden soll, stellen eben auch alle an das Internet angeschlossenen Systeme in Autokratien Teile der globalen Verwundbarkeitskette dar, die es somit ebenfalls zu stärken gilt. Im Sinne der Arbeit wäre hier zu verhindern, dass im Rahmen dieses Informationsaustauschs autokratische IT-Unternehmen zu den Proxys ihrer Regierungen werden und somit den eigentlichen Zweck des Arrangements unterwandern könnten.

Das Beispiel der israelischen NSO-Group hat ferner gezeigt, dass eine effektivere Kontrolle von Exportregeln betreffend Spionage-Software dringend nötig ist. Diese Technologien sollten nur an Länder geliefert werden, die sie nicht zu innerstaatlicher Repression/Überwachung (aus)nutzen. Dass dies auch Mitgliedstaaten der EU sein können, zeigten die Enthüllungen um den Missbrauch der Pegasus-Software in Spanien, Polen und Ungarn. Demokratische Technologie-Exportländer wie Israel sollten ihren Status nicht zur Erreichung außenpolitischer Ziele instrumentalisieren, sofern dadurch der ideelle Grundkonsens demokratischer Staaten unterminiert wird. Die Regulation des Exports potenziell schadhafter Software sollte zudem trotz bestehender Herausforderungen durch Dual-Use-Technologien allgemein gestärkt werden. Diverse Forschungsarbeiten der letzten Jahre haben sich zunehmend hiermit auseinandergesetzt und z.B. Modelle vorgeschlagen, um die Bewertung einer Software als ›Cyberwaffe‹ bereits *vor* deren Nutzung zu ermöglichen (vgl. Reinhold und Reuter 2021). Weitere seitens der Forschung diskutierte Regulationsmöglichkeiten im offensiven Cyberbereich stellen u.a. die Überlegungen zu einem ›International Vulnerabilities Equities Process‹ (IVEP) dar (Schulze 2020). Die dabei betonte Einschränkung des Nutzens einer Fokussierung auf Zero-Day-Exploits, da dies nur einen kleinen Teil aller Cyberoperationen beträfe, wird auch seitens des HD-CY.CON bestätigt, der lediglich in 38 der 1265 erfassten Fälle berichtete Zero-Days kodiert hat. Regulierungsbemühungen sollten sich somit vor allem auch auf ›Alltags-N-Day-Lücken‹ konzentrieren, die bereits bekannt sind, aus unterschiedlichen Gründen jedoch immer noch von zahlreichen AngreiferInnen gegen verschiedene Zielsysteme ausgenutzt werden können (Beispiel: WannaCry 2017).