Der vorliegende Beitrag wurde beim Deutschen Studienpreis 2023 mit dem 2. Preis in der Sektion Sozialwissenschaften ausgezeichnet. Er beruht auf der 2022 an der Universität Heidelberg eingereichten Dissertation „Proxys im staatlichen Cyberkonfliktaustrag: Eine vergleichende Analyse der VR China, Russlands, der USA und Israels“ von Dr. Kerstin Zettl-Schabath.

„Same same but different“ – Warum und wofür Autokratien und Demokratien im Cyberspace auf nichtstaatliche Akteure setzen und wie dies unsere Cyber(un)sicherheit beeinflusst

Wer regiert die Cyberwelt?

Kaum ein Tag vergeht, an dem Medien, IT-Unternehmen oder staatliche Behörden nicht von neuen Bedrohungen im Cyberspace berichten. In Zeiten zunehmender Vernetzung, Innovationen wie dem Internet-of-Things, Smart-Home-Systemen und autonom fahrenden Autos, ist das Thema der „Cyber(un)sicherheit“ von drängender Relevanz für sämtliche Akteursgruppierungen. Cyberangriffe bedrohen längst nicht mehr „nur“ wirtschaftliche Interessen, z.B. durch Wirtschaftsspionage. Sie werden stattdessen auch gegen politische Akteure in Friedens- und Konfliktzeiten, aber auch gegen die Zivilgesellschaft, z.B. von autokratischen Regimen, eingesetzt. Hinzu kommt die Vernetzung von Steuerungsanlagen im Energiesektor, Krankenhäusern und weiteren Einrichtungen, die für das Funktionieren einer Volkswirtschaft sowie die physische Unversehrtheit aller Menschen unabdingbar sind. Als besondere Bedrohung haben sich in den letzten Jahren sog. „Ransomware-Operationen“ heraus entwickelt, also Schadsoftware, die die Daten eines gehackten Zielsystems verschlüsselt und meist nur gegen Lösegeldzahlungen wieder entschlüsselt. Eine solche Attacke legte im Mai 2021 das US-Unternehmen Colonial Pipeline, und damit die Ölversorgung weiter Teile der USA, zeitweise lahm. Diese steigende Bedrohungsdynamik setzte somit nicht erst im Februar 2022 ein, als Russland seinen Angriffskrieg auf die Ukraine startete und wie zuvor bereits auch u.a. auf Cyberangriffe als Konfliktmittel setzt(e). LeserInnen solcher Schlagzeilen könnten annehmen, dass der Cyberraum eine regelloser „Wilder Westen“ sei, in dem Staaten rücksichtslos immer schwerwiegendere Hacking-Operationen ausüben. Längst finden sich Cyberangriffe in Jahresberichten von Sicherheitsbehörden auch in Deutschland ganz oben auf der Liste der dringlichsten Bedrohungsformen.

Ein Blick in die Cybersicherheitsforschung setzt dem Narrativ des eskalierenden Cyberkonfliktaustrags gegenteilige Befunde entgegen: „Cyber war will not take

place“ schlussfolgerte der Politikwissenschaftler Thomas Rid bereits 2012. So seien strukturelle Unterschiede der digitalen zur analogen Sphäre ursächlich dafür, warum auch in absehbarer Zukunft kein tatsächlicher „Cyberkrieg“, mit durch Cyberangriffe hervorgerufenen Toten und Verletzten, zu erwarten sei. Die vornehmlich in der Wissenschaft geführte Debatte um staatliche „Zurückhaltung“ im Cyberspace arbeitete sich besonders an folgenden Strukturmerkmalen des Cyberspace ab: 1) der stärkeren Anonymität der Angreifer als im analogen Raum, mit einer damit verbundenen erschwerten Verantwortungszuweisung (Attribution) für Cyberangriffe, 2) den unklaren „Erfolgen“, die Cyberangriffe mit sich bringen, da Angreifer nur sehr schwer die tatsächlichen Auswirkungen ihrer Operationen auf die anvisierten Ziele antizipieren können, 3) der oftmals nachteiligen Kosten-Nutzen-Rechnung von Cyberoperationen im Gegensatz zu traditionellen Konfliktaustragungsmitteln und 4) der ebenfalls mit der unklaren Ursache-Wirkungs-Beziehung verbundenen Gefahr, dass ein Hack auch die Systeme des Angreifers selbst treffen kann.

Diese Merkmale können nicht nur den bislang ausgebliebenen „Cyberkrieg“ erklären, sondern auch, warum der Ruf nach immer offensiveren Kompetenzen für Sicherheitsbehörden im Cyberspace aus gesamtgesellschaftlicher Sicht wenig sinnvoll ist. Die Wirkung von sog. „Hack-Backs“ ist nach wie vor umstritten, deren Schadenspotenzial für das allgemeine IT-Sicherheitsniveau jedoch in Zivilgesellschaft und Forschung umso anerkannter.

Weniger Aufmerksamkeit erfuhr bislang die Rolle von nichtstaatlichen Akteuren im Rahmen dieser Zurückhaltungsdebatte, obwohl *Hacktivisten* und *Cyberkriminellen* erhebliche Handlungsmöglichkeiten im digitalen Raum seitens der Forschung attestiert wurden. Könnte es also sein, dass neben den genannten Faktoren besonders auch nichtstaatliche Akteure, sowohl aufseiten der Angreifer als auch aufseiten der Opfer, zu dem seit Jahren verzeichneten „unruhigen Cyberfrieden“ beitragen? So gibt es immer häufiger und oft auch immer komplexere Cyberoperationen, die eine steigende Anzahl an Staaten und nichtstaatlichen Akteuren ausüben, ohne dabei die kritische „Cyberwar“-Schwelle zu überschreiten.

Autokratische & demokratische „Cyber-Proxys“: Same same but different?

Aufgrund der varianten innerstaatlichen Strukturen und oftmals unterschiedlichen Außenpolitiken setzen autokratische Staaten wie Russland oder China sog. „Cyber-Proxys“ vermutlich anders ein als Demokratien. Cyber-Proxys sind nichtstaatliche Akteure, die stellvertretend/im Auftrag von Regierungen offensive oder defensive Handlungen im Rahmen von Cyberkonflikten ausüben. Wer nutzt jetzt aber wen

und wofür? Und lassen sich trotz Unterschieden zwischen den Regimetypen auch Gemeinsamkeiten erkennen?

Da ich davon ausgehe, dass nichtstaatliche Akteure Verantwortlichkeiten beider Regimetypen im Rahmen von Cyberkonflikten verschleiern (sollen), jedoch auf unterschiedliche Art und Weise, widmet sich meine Dissertation diesen Fragen:

Warum nutzen Autokratien und Demokratien gleichermaßen private Akteure im Rahmen von Cyberkonflikten? Tun sie dies auf unterschiedliche Art und Weise, und wie lässt sich dies durch den jeweiligen Regimetyp erklären?

Die systematische und auf Grundlage einer breiten Datenbasis erfolgende Beantwortung dieser Fragen verspricht ein wichtiges Puzzleteil zu sein, um die skizzierte, eben noch nicht vollends eskalierte Cyberkonfliktdynamik zu erklären. Für Demokratien ist ein tieferes Verständnis autokratischer Cyberkonfliktstrategien unabdingbar. Ist deren besonders durch innenpolitische Einflussfaktoren geprägte Motivlage für die Durchführung unterschiedlicher Cyber-Proxy-Operationen klar, kann man diese künftig auch besser antizipieren, abwehren oder darauf reagieren. Gleichzeitig erfordert das liberal-rechtsstaatliche Selbstverständnis demokratischer Staaten eine schonungslose Analyse der eigenen „Cyberbilanz". So ging ich in meiner Arbeit *nicht* davon aus, dass die USA oder Israel regelmäßig nichtstaatliche Akteure zur *finalen* Durchführung von Hacking-Operationen nutzen. Eine Aufweichung des staatlichen Gewaltmonopols wäre in den meisten liberal-demokratischen Staaten verfassungsrechtlich verboten. Für Demokratien entwickelte ich ein Theoriemodell staatlicher Cyber-Proxy-Nutzung für *defensive* Handlungen wie die Attribution von Cybervorfällen. Diese Annahme fußt auf folgenden Thesen:

1. Demokratien sehen sich dem öffentlichen Kenntnisstand nach weitaus häufiger autokratischen Cyberangriffen ausgesetzt als umgekehrt, da sie hierfür aufgrund ihrer meistens stärkeren Digitalisierung und Vernetzung sehr viel anfälliger und verwundbarer sind.

2. Demokratien schrecken dennoch regelmäßig davor zurück, *selbst* einen Cyberangreifer als solchen zu benennen (zu attribuieren).

Demokratien attribuieren nicht gerne selbst, aufgrund ihrer größeren Verwundbarkeit und weil einer Attribution auch eine Reaktion folgen muss: Lastet Olaf Scholz eine Cyberattacke auf deutsche Systeme öffentlich dem Kreml an, erwarten die Bevölkerung sowie weite Teile des politischen Systems auch eine entsprechende Reaktion. Die Merkmale des Cyberspace machen es politischen EntscheidungsträgerInnen jedoch schwer, mit sinnvollen, d.h. effektiven, demokratisch und rechtsstaatlich legitimierten und für die eigene Bevölkerung unbedenklichen „Cyber-Reaktionsoptionen" aufzuwarten. Da man autokratische Cyberangreifer dennoch

wissen lassen will, dass ihre Handlungen nicht unentdeckt bleiben, übernahmen in der Vergangenheit regelmäßig private IT-Unternehmen die Aufgabe der öffentlichen Attribution von Cyberangriffen. Defensive Cyber-Proxys dien(t)en demokratischen Regierungen also dazu, ihre eigentliche Verantwortung zum Attribuieren und Handeln in einem solchen Falle zu verschleiern und ihnen mehr Handlungsspielraum zu gewähren.

Das demokratische „Handlungsdilemma“ trat auch in der Debatte um Deutschlands Leopard-Panzer-Lieferungen an die Ukraine zutage. Demokratien sehen sich sehr viel stärker als Autokratien domestischen, aber auch externen Interessen unterschiedlicher AkteurInnen ausgesetzt. Das in der Öffentlichkeit als „Zaudern“ beschriebene Vorgehen der Bundesregierung könnte im Sinne der Dissertation ebenfalls als eine Art Verschleierungstaktik der eigenen Verantwortlichkeit gewertet werden, um sich so lange zeitlichen Spielraum zu verschaffen, bis die USA ebenfalls zu eigenen Panzerlieferungen bereit waren. Übertragen auf die Attribution von Cyberangriffen bedeutet dies, dass private IT-Unternehmen so lange für Demokratien die öffentliche Verantwortungszuweisung übernehmen können, bis die Regierung z.B. eigene Attributionskoalitionen geschmiedet hat und die Risiken einer Eskalation auf mehrere Schultern verteilen kann.

Im Gegensatz dazu haben Autokratien ein großes Interesse daran, offensive Cyberoperationen gegen Demokratien durchzuführen, die eigene Verantwortlichkeit jedoch ebenfalls zu verschleiern. Aufgrund ihrer geringeren Verwundbarkeit im Cyberspace, sowie ihrer Unterlegenheit im konventionell-militärischen Bereich (beachtet man militärische Bündnisse wie die NATO), befinden sie sich gegenüber Demokratien besonders in Cyberkonflikten in einer asymmetrischen, zu ihrem Vorteil ausgestalteten Interdependenzsituation. Gemäß der Theorie des „Neuen Liberalismus“ nach Andrew Moravcsik verfügen aber auch Autokratien über unterschiedliche „Präferenzkonstellationen“: In Einparteienregimen wie der Volksrepublik China können andere Akteure ihre Interessen durchsetzen als in personalistischen Regimen wie Russland. Gleichzeitig sollen unterschiedliche Cyberoperationsformen den eigenen Machterhalt sichern. Ist für eine Autokratie die wirtschaftliche Modernisierung der Schlüssel zum eigenen Machterhalt, werden ihre Cyber-Proxys auch eher auf Cyberspionage, denn auf disruptivere Operationen setzen. Legitimiert sich eine Autokratie dagegen vor allem durch den ideologisierten Personenkult um ihren Anführer, dürften informationsbasierte Cyberangriffe, wie z.B. Hack-and-Leak-Operationen gegen „Regimefeinde“, ein Mittel der Wahl sein.

In Autokratien bedroht oft nicht das eigene Volk, sondern konkurrierende Elitengruppen das herrschende Regime. Eine zivile autokratische Regierung wird daher z.B. dem Militär nicht zu viel offensive Cyberfähigkeiten übertragen wollen,

aufgrund der stets bestehenden Coup-Gefahr. Der Einsatz von (offensiven) Cyber-Proxys kann somit auch diese innenpolitische Gefahr reduzieren.

HD-CY.CON als erster politikwissenschaftlicher Cyberkonfliktdatensatz seiner Art

Zusammenfassend untersucht meine Dissertation staatliche Cyber-Proxy-Nutzungsmuster, basierend auf der Grundannahme, dass Regierungen regelmäßig die Kosten, die mit offensiven (Autokratien) oder defensiven (Demokratien) Handlungen im Cyberspace verbunden sind, delegieren möchten. Der Neue Liberalismus ermöglicht die getrennte Untersuchung des Einflusses ökonomischer, ideeller sowie institutionenbasierter Präferenzen von Staaten und welchen Einfluss diese auf deren Cyberkonfliktverhalten von 2000 bis 2021 hatten.

Der sog. „Heidelberger Cyberkonfliktdatensatz“ (HD-CY.CON) bildet die Grundlage für meine vier empirischen Fallstudien. Als hauptverantwortliche Mitarbeiterin habe ich diesen in einem von der Deutschen Stiftung Friedensforschung geförderten Projekt mit erstellt (2019 – 2021). Der HD-CY.CON stellte zum Zeitpunkt seiner Veröffentlichung den umfänglichsten, mit 43 Kategorien ausgestatteten Datensatz über Cyberkonflikte mit politischer Dimension dar. Er umfasst 1265 Cybervorfälle und kategorisiert sie zu Themen wie Attributionen, ihrer Intensität sowie Verschränkungen mit bestehenden konventionellen Konflikten. Meine Arbeit brach mit dem vorherrschenden Fokus der Cyberkonfliktforschung auf Einzelfall oder allenfalls vergleichenden Untersuchungen mit sehr geringer Fallzahl, indem ich für jeweils zwei Autokratien und Demokratien deren Cyberkonfliktverhalten umfassend analysieren konnte. Die zentrale Bedeutung, die gerade politische EntscheidungsträgerInnen der systematischen, konsistenten und interdisziplinären Datengenerierung über Cyberkonflikte beimessen, verdeutlicht die Weiterführung des HD-CY.CON im Rahmen des Projekts „European Repository of Cyber Incidents“ (EuRepoC). Gegenwärtig durch das Auswärtige Amt und das dänische Außenministerium gefördert, vereint EuRepoC neben dem federführenden Institut für Politische Wissenschaft der Universität Heidelberg noch Konsortialpartner aus drei verschiedenen Ländern, aus den Bereichen der Politikwissenschaft, des Völkerrechts sowie der IT-Forensik. Auf der Projektwebpage veranschaulicht u.a. ein interaktives Dashboard Cyberkonfliktdynamiken von 2000 bis heute. Eine individuell konfigurierbare Tabellenansicht über alle in der Datenbank erfassten Cybervorfälle erlaubt den Detailblick auf die mittlerweile über 60 interdisziplinären Kategorien.

Russischer „Cyber-Bully“ vs. chinesischer „Cyber-Spy“

Der Datensatz verzeichnete für China und Russland eine hohe Anzahl an Cyber-Proxy-Operationen, sowie auch direkt-staatlichen Akteuren angelasteten Vorfällen. Die anvisierten Ziele und Operationsformen offenbarten jedoch auch hinreichende Unterschiede zwischen den beiden Ländern. Russlands Cyber-Proxy-Strategie basierte sehr viel stärker auf informationsbasierten, disruptiveren Operationsformen, die mehr „Lärm“ erzeugten als die dominierende chinesische Cyberspionage. Zugleich setzte Russland in der Vergangenheit auf Cyberkriminelle als Proxys, denen man im Gegenzug Straffreiheit gewährte. Die VR China rekrutierte ihre Proxys dagegen häufiger aus inländischen Technologieunternehmen. Erklären können dies der jeweilige Regimetyp sowie die historisch bedingte Verfügbarkeit unterschiedlicher Proxy-Typen: Während Russland nach dem Ende der UdSSR viele Informatiker ohne Jobperspektiven beheimatete, strebte China bereits seit dem Ende der Mao-Diktatur nach wirtschaftlicher Entwicklung und vor allem Modernisierung, z.B. durch den Aufbau einheimischer Technologieunternehmen. Während russische Cyberoperationen unter Putin insbesondere politische Gegner, demokratische Werte und Institutionen schwächen sollten, verfolgte China eine Strategie der wirtschaftlichen Modernisierung durch den Diebstahl geistigen Eigentums. Verantwortlich hierfür waren die zentralen Interessen der russischen Elitegruppierung der „Silowiki“ um Wladimir Putin auf der einen und die der Kommunistischen Partei Chinas auf der anderen Seite. Als intervenierende Variable untersuchte die Arbeit zudem den Einfluss konventioneller Konflikte auf die Cyber-Proxy-Nutzung: Russland führte besonders im bereits gewaltsamen Ukraine-Konflikt auch schwerwiegendere Cyberoperationen als in noch nicht gewaltsam eskalierten Konflikten aus. China setzt(e) auch im Kontext konventioneller Konflikte wie um das Südchinesische Meer dagegen noch auf Cyberspionage, was sich etwa gegenüber Taiwan künftig ändern könnte. Gemäß dem entwickelten liberalen Erklärungsmodells nutzten die beiden Länder Cyber-Proxys, um eigene Verwundbarkeiten auf der wirtschaftlichen Ebene, oder die ideellen Verwundbarkeiten politischer Kontrahenten systematisch zu manipulieren.

Amerikanische „Cyberoffensive“ vs. israelische „Cyberambivalenz“

Attributionen von US- und israelischen IT-Unternehmen wurden mit Abstand am häufigsten im HD-CY.CON erfasst. Beide Länder sind im Technologiebereich führend, sodass diese auch besonders oft Opfer von Cyberangriffen wurden. Die USA stellen für Länder wie China, Iran und Nordkorea ein attraktives Ziel ökonomisch motivierter Cyberspionage dar, um geltende Wirtschaftssanktionen zu umgehen. Russland greift die USA vor allem an, um sie als Symbol der liberal-demokratisch geprägten Staatengemeinschaft innenpolitisch mithilfe von Cyberangriffen zu

schwächen. Israel stellt dagegen aufgrund seiner Involvierung in regionale Konflikte nicht nur für Wirtschaftsspionage, sondern auch für disruptivere Operationen ein häufiges Ziel dar.

Für die USA ließ sich die weitaus schwerer nachzuvollziehende demokratische Staat-Proxy-Beziehung besonders dann begründen, wenn die Attributionen der IT-Unternehmen Cyberoperationen adressierten, die die drängendsten Verwundbarkeiten der USA ausnutzten. Im Gegensatz zur offensiven Cyber-Proxy-Nutzung autokratischer Staaten ließ sich die *aktive* Beauftragung/Unterstützung privatwirtschaftlicher Attributionen durch staatliche Stellen für beide Demokratien schwerer belegen. Für Demokratien kann von einer passiveren Staat-Proxy-Beziehungsform ausgegangen werden, die grundlegend auf der gegenseitigen Abhängigkeit voneinander beruht. Auch private IT-Unternehmen sind auf politische Unterstützung demokratischer Regierungen angewiesen. Unter Donald Trump setzte die USA als Antwort auf Cyberoperationen besonders auf die „Attribution by indictment"-Strategie. Eine Vielzahl von Anklagen wurde gegen ausländische Hacker erhoben, ohne jedoch reelle Aussichten auf eine tatsächliche Strafvollstreckung zu haben. Hierdurch konnte zwar „Täterwissen" öffentlich gemacht werden, ohne aber wirklich schwerwiegendere und mit politischen Kosten verbundene Reaktionsoptionen anwenden zu müssen. Hinzu kamen eine Reihe an offensiven Cyberoperationen staatlicher US-Akteure, die an die Medien bewusst durchgestochen, jedoch nicht offiziell kommuniziert wurden. Auch dieses Vorgehen stellt eine Verantwortungsverschleierung demokratischer Akteure dar.

Im Gegensatz zu den USA attribuierten israelische PolitikerInnen keinen Cyberangriff öffentlich. Dies übernahmen stattdessen israelische IT-Unternehmen vor allem für Operationen, die von Israels größten Bedrohungen, dem Iran sowie palästinensischen Gruppierungen, ausgeübt wurden. Aufgrund der sehr engen Verbindung zwischen öffentlichem und privatem Sektor in Israel ist hier noch stärker von einer stetigen Attributionskoordination zwischen IT-Unternehmen und staatlichen Stellen als in den USA auszugehen. „Quasiattributionen" israelischer EntscheidungsträgerInnen, in denen das hohe Maß an Cyberangriffen gegen Israel *allgemein* öffentlich thematisiert wird, spiegeln Israels historisch gewachsene „strategische Ambivalenz" wider: So hat das Land öffentlich bislang nie bestätigt, Atomwaffen zu besitzen, signalisiert genau dies informell jedoch immer wieder. Dies stellt ein erhebliches Legitimationsproblem dar, gerade wenn Prinzipien der transparenten, verantwortlichen und rechtsstaatlichen Regierungsführung untergraben werden. Bemerkenswert ist für beide untersuchte Demokratien, dass diese Verschleierungstaktiken mit einer zunehmenden gesamtgesellschaftlichen Polarisierung einhergingen.

Die „Demystifizierung“ von Cyberangriffen, als stärker politisches denn militärisches Mittel, gewinnt immer größere Bedeutung. Nur wenn die innenpolitischen Dynamiken und Strukturbedingungen aufseiten der Offensive *und* Defensive umfassend analysiert werden, können auch Aussagen über die tatsächliche Effektivität von Cyberabwehrmaßnahmen getroffen werden. Nicht jedes Land ist gleich anfällig für unterschiedliche Cyberoperationsformen; nicht jeder offensiv agierende Staat wählt dieselben Cyberoperationsformen zur Erreichung seiner Ziele aus, und gleichermaßen unterhalten Staaten auch individuell geprägte Beziehungen zu ihren nichtstaatlichen Akteuren. Die besondere gesellschaftspolitische Relevanz des Themas der Arbeit zeigt sich auch in ihrer bisherigen Resonanz, etwa durch die Verleihung des Preises „Frieden – Freiheit – Sicherheit“ der Dr. Karl A. Lamers Friedens-Stiftung. Zugleich demonstrieren die politische Unterstützung des EuRepoC-Projekts als Weiterführung des HD-CY.CON-Datensatzes sowie das große Interesse von Industrie, Zivilgesellschaft und Wissenschaft, dass das systematische Kartografieren von Cyberkonfliktdynamiken gebotener ist denn je.