Quelle: © Kacper Pempel, Reuters.

Globale Machtverschiebungen

Digitale Technologie als neue Machtressource

Konflikte im virtuellen Raum

Jason Chumtong / Christina Stolte

Digitale Fähigkeiten gewinnen in der internationalen Politik zunehmend an Bedeutung. Staaten, die in der Lage sind, Cyberoperationen durchzuführen, können ihren internationalen Gestaltungsspielraum deutlich erweitern. Dies gilt in besonderer Weise für kleine und mittlere Staaten, die über geringe traditionelle Machtressourcen verfügen. Denn mithilfe von Cyberfähigkeiten können sie auch mächtigere Staaten empfindlich schwächen.

Unsichtbare Machtverschiebungen

In den letzten 20 Jahren haben sich mit dem Aufstieg Chinas und anderer Schwellenländer tektonische Verschiebungen im globalen Machtgefüge vollzogen.[1] Saßen die heutigen Global Player zu Beginn der Jahrtausendwende noch am Katzentisch der Weltpolitik und waren von internationalen Abstimmungs- und Entscheidungsprozessen weitgehend ausgeschlossen, so sind Entscheidungen von globaler Tragweite heute ohne Staaten wie China oder Indien kaum mehr vorstellbar. Besonders augenscheinlich wird der rasante Aufstieg dieser einstigen Entwicklungsländer im wirtschaftlichen und militärischen Bereich: Vordere Rangplätze in Bezug auf Wirtschaftsgröße, Wachstum, Militärausgaben und Technik demonstrieren den beeindruckenden Machtzuwachs. Glitzernde Wolkenkratzer, Nukleartechnik und spektakuläre Weltraummissionen verkünden die Botschaft von der neuen Stärke – und lassen kaum ein gängiges Machtsymbol des späten 20. Jahrhunderts aus, um die neu gewonnenen Kapazitäten und den Statusgewinn sichtbar zur Schau zu tragen.

Eine Machtverschiebung weniger sichtbarer Art hat sich – fast unbemerkt von der Weltöffentlichkeit, weil still und unsichtbar und ohne sichtbare Demonstration der Stärke – parallel vollzogen: die Machtverschiebung im digitalen Raum.[2] So hat eine Reihe von Staaten innerhalb der letzten Dekade verstärkt auf den Auf- und Ausbau ihrer digitalen Fähigkeiten gesetzt und damit neue Wege gefunden, internationale Entscheidungen und Ereignisse im Sinne ihrer Interessen zu prägen und so Macht auszuüben.

Ähnlich wie beim Aufstieg des globalen Südens handelt es sich um eine sehr überraschende und vergleichsweise zügige Machtverschiebung, die sich binnen weniger Jahre ereignet hat. Dies liegt zum einen daran, dass der Cyberspace – definiert als virtueller Raum, der alle durch das Internet weltweit erreichbaren Informationsstrukturen umfasst – insgesamt eine neue Sphäre staatlichen Handelns ist. Zum anderen liegt der Überraschungseffekt in der ungewöhnlichen Ausprägung dieser Machtsphäre begründet, die – anders als die klassischen Felder des zwischenstaatlichen Wettbewerbs um Macht und Einfluss wie etwa die militärische Stärke oder die Wirtschaftskraft sowie der Wohlstand eines Landes – nur schwer quantifizierbar und selten wirklich sichtbar ist. Doch auch wenn es sich daher um eine unsichtbare, kaum greifbare Form der Macht handelt, erfüllt sie dennoch die traditionelle Definition als „Mittel zur Interessensdurchsetzung“[3] gegenüber einem anderen Staat, wie etwa im National Cyber Power Index argumentiert wird.[4] So können mithilfe von Cyberspionage oder Cyberangriffen erhebliche finanzielle oder gar humanitäre Schäden in anderen Staaten verursacht werden. Doch auch schon simple Einflusskampagnen können mit digital verstärkter Stimmungsmache und gezielter Falschinformation die Vertrauenswürdigkeit oder sogar Stabilität der Ordnung eines verfeindeten Staates gefährden und den Gegner empfindlich schwächen.[5]

Auch in der analogen Welt gab es und gibt es eine „unsichtbare“ Sphäre der Konfliktaustragung, und zwar im Bereich der Nachrichtendienste. Kleine und mittlere Mächte kompensieren dabei geringere militärische Stärke durch umfassende Geheimdiensttätigkeit. Der digitale Machtkampf

auf zwischenstaatlicher Ebene kann deswegen auch als Erweiterung dieser Sphäre betrachtet werden, denn die Schwelle zum Einstieg ist niedrig. Wenngleich Begriffe wie *Cyber Powers* Assoziationen von technologisch führenden, fortschrittlichen Staaten wecken, so sind unter den neuen digitalen Mächten nicht nur bekannte Global Player, sondern auch Staaten, die auf den traditionellen Feldern des zwischenstaatlichen Kräftemessens keine herausragenden Fähigkeiten aufweisen.

Die Anwendung digitaler Technologien eröffnet Staaten ohne traditionelle Machtressourcen Möglichkeiten, internationale Politik in ihrem Sinne zu beeinflussen.

So spielen bedeutende Großmächte wie die USA oder China auch auf dem Feld der digitalen Machtausübung nach wie vor die wichtigste Rolle.[6] Doch während der digitale Raum für die etablierten Großmächte lediglich eine weitere Sphäre ist, in der sie ihre Interessen durchsetzen und Macht ausüben, bietet die Anwendung digitaler Technologien kleineren Staaten ohne traditionelle Machtressourcen ganz neue Möglichkeiten, um internationale Politik in ihrem Sinne zu beeinflussen und ihre Interessen offensiv zu verfolgen. Neben der oben konstatierten Machtverschiebung hin zum digitalen Raum, der gegenüber dem klassisch militärischen Bereich stark an Bedeutung gewonnen hat, vollzieht sich somit noch eine weitere Machtverschiebung hin zu jenen Staaten, die das Potenzial von Cyberfähigkeiten früh als Machtressource entdeckt und für sich erschlossen haben.

Im Folgenden sollen Russland, Venezuela und Iran als aufstrebende digitale Mächte beleuchtet werden. Anhand der Fallauswahl von Staaten verschiedener Machtkategorien soll das breite Spektrum und die Vielfalt dieser neuen Machtform aufgezeigt und das Bewusstsein für die Möglichkeiten geschärft werden, die sich nicht nur für technologisch führende Cybermächte, sondern auch für Staaten aus der zweiten und dritten Reihe der internationalen Politik durch diese neue Machtressource bieten.

Das Internet als zwischenstaatlicher Konfliktraum

Um zu verstehen, welche Rolle der Cyberspace als Sphäre für internationale Machtkämpfe und Konflikte einnimmt, hilft ein Blick auf die verschiedenen Stufen zwischenstaatlicher Konflikte in der analogen Welt. Angenommen, Akteur A weist den Botschafter von Akteur B aus, und dieser reagiert nicht mit der Einbestellung des Botschafters, sondern lässt Panzer an die Landesgrenze fahren. Wenn Akteur A im Gegenzug ebenfalls mit einer „schärferen" Maßnahme reagiert und beispielsweise Warnschüsse auf die Panzer abgibt, eskaliert die Auseinandersetzung von der diplomatischen auf die militärische Ebene. Die Maßnahmen in diesem zwischenstaatlichen *Tit for Tat* nehmen also an Aggression immer weiter zu. In der Konflikttheorie werden solche Entwicklungsstufen auf sogenannten Eskalationsskalen oder Eskalationsleitern abgebildet.[7] Sie sollen aufzeigen, welcher Angriffsmodus mit welcher Konfliktintensität korrespondiert. Auch die Variabilität von Cyberattacken ist, wie im Folgenden zu sehen, auf einer Skala darstellbar.

Die Eskalationsskala von Cyberattacken:[8]

Stufe 1	Vorbereitung: Rekrutierung und Ausbildung von Hackern; Vorbereitung von Angriffen
Stufe 2	Geringe Schikane: Beeinflussung von Informationsräumen durch Propaganda und Fake News; Cyberspionage und Datenraub via Trojaner
Stufe 3	Schwere Schikane: temporäre Stilllegung von Dienstleistungen via DDoS-Angriffe (Distributed Denial of Service); Swatting (Fehlalarmierung von Notfallpersonal, Polizei, Feuerwehr, Notarzt)

Stufe 4 Geringer Schaden: Zerstörung von kritischen Daten; gezielte Angriffe auf militärische Infrastruktur via Schadsoftware (z. B. Stuxnet)[9]

Stufe 5 Schwerer Schaden: gezielte Beeinträchtigung militärischer Fähigkeiten, Zerstörung militärischer Infrastruktur (bislang kein Beispiel)

Stufe 6 Schwerwiegender/katastrophaler Schaden: permanenter Schaden an der Zivilbevölkerung durch die Zerstörung ziviler Infrastruktur (bislang kein Beispiel)

Stufe 7 Existenzgefährdender Schaden: Schaden im Ausmaß eines nuklearen Erstschlages (bislang kein Beispiel)

Intuitiv bietet der Cyberspace zwar viel Eskalationspotenzial für zwischenstaatliche Konflikte, insbesondere, weil durch die digitale Vernetzung jede Verbindung mit dem Internet eine potenzielle Schwachstelle ist und somit einen Angriffsvektor bietet. Gleichwohl sind Cyberangriffe unattraktiv für Gegenschläge mit höherer Intensität – und zwar aus folgenden Gründen:

1. Cyberangriffe sind nicht zielagnostisch. Während konventionelle Waffen ohne große Anpassung gegen eine Vielzahl unterschiedlicher Ziele angewandt werden, benötigen Cyberangriffe eine individuelle Anpassung auf das Ziel. Grundsätzlich kann eine Rakete sowohl gegen ein Gebäude als auch ein Fahrzeug mit absehbarem Detonationsschaden abgeschossen werden.[10] Der Trojaner für das System X funktioniert jedoch in der Regel nicht beim System Y.

2. Cyberangriffe sind unflexibel. Aufgrund der hohen Dichte an unterschiedlichen (Betriebs-)Systemen, die in der Welt der Informations- und Telekommunikationstechnologie zum Einsatz kommen, nimmt die Auswahl des Angriffsvektors und die Entwicklung eines passenden Angriffes viel Zeit in Anspruch. Chris Inglis, ehemaliger stellvertretender Direktor der NSA, bestätigt, dass ein Cyberangriff zu 90 Prozent aus Vorbereitung besteht. Für schnelle Gegenreaktionen sind Cyberangriffe ungeeignet.[11]

3. Cyberangriffe sind kurzlebig. Da Software als nicht-physische Komponente einer Technologie relativ wenige Ressourcen zur Weiterentwicklung verbraucht, ist der Cyberspace einer hohen Frequenz an dynamischen Veränderungen ausgesetzt. Erfolgreiche Cyberangriffe beschleunigen dabei den Prozess der Weiterentwicklung, da als Reaktion die ausgenutzten Softwareschwachstellen langfristig behoben werden. Der Offensivmythos besagt, dass bei Cyberangriffen der Angreifer immer im Vorteil gegenüber dem Verteidiger ist. Dies kontert Paul Nakasone, Direktor der NSA, mit dem Fakt, dass offensive Cyberfähigkeiten durchschnittlich nicht länger als sechs Monate wirksam sind.[12]

Cyberangriffe bewegen sich in einer völkerrechtlichen Grauzone.

Vor diesem Hintergrund wird deutlich, dass der Mehrwert von Cyberangriffen hauptsächlich in ihrer Nutzung zur Beeinflussung eines feindlichen Informationsraums und in der verdeckten Unterwanderung von Informationsnetzwerken liegt.[13] Sie sind in ihrem Wesen damit klassische Methoden der Spionage und Manipulation, besitzen aber weniger Vorteile für den traditionellen Angriff, sondern unterstützen vielmehr moderne Militäroperationen.[14] Entgegen der Clausewitzschen Dichotomie von Krieg und Frieden bewegen sich Cyberangriffe in einer völkerrechtlichen Grauzone.[15] Insbesondere niedrigschwellige Cyberoperationen bieten für angreifende Staaten aber gerade deshalb Spielraum für die Stärkung ihres Einflusses, da es sich nicht um einen offen erklärten Krieg handelt und die konkrete Gefahr eines eskalierenden Gegenschlags gering ist. Dies ist insbesondere gegenüber militärisch mächtigeren Staaten ein entscheidender Faktor.

Von *Cyber Superpowers* und *Rising Cyber Powers*: Das Spektrum digitaler Machtausübung

Wesentliche Ursachen für den Erfolg von Cyberangriffen sind nicht notwendigerweise die Komplexität von Schadsoftware oder die Qualität der zur Verfügung stehenden Ressourcen und Fähigkeiten des Personals. Entscheidend für die Effektivität der Spionagearbeit ist die Infiltration der Systeme über einfachste Methoden zur Beschaffung von Passwörtern und damit zu immer mehr Zugängen. Das Öffnen einer Phishing-Mail oder das Benutzen von infizierten USB-Sticks sind gern genutzte Einfallstore und anschauliche Beispiele dafür, wie einfach Schadsoftware ins System gelangt, denn oftmals ist die Schwachstelle im Cyberspace der Mensch und nicht das System. Der leichtsinnige Umgang mit dem Internet, das Benutzen von Werkspasswörtern bei Netzwerkroutern, die Wiederbenutzung privater Passwörter für berufliche Anwendungen oder gar das Aufschreiben ganzer Zugangsdaten in Textdateien oder E-Mails gehören zu den entscheidenden Schwachstellen, die in Cyberoperationen maßgeblich dazu beitragen, den digitalen Angriff zu lancieren. Die nachfolgenden Beispiele aus Russland, Iran und Venezuela zeigen, in welchem Umfang Cyberangriffe bereits zur Manipulation der internationalen Machtverhältnisse zum Einsatz kommen.

Russland

Als klassische Großmacht und einstige Supermacht im Zweikampf mit den USA zählt Russland nicht zu den Überraschungskandidaten im Cyberspace. Russland hat in der letzten Dekade enormen Kraftaufwand in die Rückgewinnung seines alten Status investiert und militärisch aufgerüstet. Dabei haben digitale Technologien und Cyberfähigkeiten früh eine zentrale Rolle eingenommen. Schon 2013 formulierte der russische Generalstabschef Walerij Gerassimow die Grundsätze des neuen Ansatzes russischer Machtprojektion, der den umfangreichen Einsatz von Desinformationen und andere nichtmilitärische Maßnahmen vorsieht und weit über Konzepte konventioneller Kriegsführung hinausgeht. Verschiedene Aspekte des Cyberkonflikts, wie etwa digitale Angriffe auf Institutionen und Infrastruktur anderer Staaten oder digital geführte Beeinflussungskampagnen zur Manipulation der politischen Willensbildung in verfeindeten Staaten, ergänzen sich hierbei zu einem ganzheitlichen Ansatz, der die im Westen lange übliche Trennung konventioneller und digitaler Kriegsführung schon früh überwand und das Potenzial dieser neuen Machtressource frühzeitig erkannte und ausschöpfte.[16]

Russlands Propagandakampagnen zielen darauf, gesellschaftlichen Unfrieden und politisches Chaos zu stiften, um Rivalen von innen heraus zu schwächen.

Russland nahm von Beginn an eine Pionierrolle im Cyberspace ein. So wird etwa der erste bekannte Cyberangriff, bei dem im Jahr 2007 Regierungsbehörden in Estlands Hauptstadt Tallinn attackiert wurden, Russland zugeschrieben. Auch die erste Cyberattacke auf kritische Energie-Infrastruktur – die gezielte Abschaltung der Energieversorgung der ukrainischen Region Ivano-Frankivsk im Jahr 2015 durch einen Hackerangriff – geht auf das Konto Russlands. In Deutschland erlangten die von russischen Geheimdiensten orchestrierten Angriffe von Hackergrupppen wie APT28, auch *Fancy Bear* genannt, mit dem Cyberangriff auf den Deutschen Bundestag 2015 sowie Institutionen der US-Regierung zwischen 2014 und 2016 erstmals größere mediale Aufmerksamkeit, da sie der Welt vor Augen führten, dass auch sicher geglaubte Regierungsinstitutionen wie das Weiße Haus den Angriffen nicht gewachsen waren. Heute blickt Russland auf 15 Jahre internationaler Cyberaktivitäten zurück und zählt neben den USA, Großbritannien, Israel und China zu den *Cyber Superpowers*.[17]

Neben den oben beschriebenen Cyberattacken, die Russland über die letzten 15 Jahre perfektioniert hat, setzt die einstige Supermacht auch

Gezielte Einflussnahme: Mit auf spezifische nationale Kontexte abgestimmten Desinformationskampagnen trägt Russland aktiv zur Polarisierung der Gesellschaften in westlichen Demokratien bei. Quelle: © Gleb Garanich, Reuters.

in einer weiteren Domäne der digitalen Kriegsführung weltweit Akzente: Globale sowie auf spezifische nationale Kontexte abgestimmte Desinformationskampagnen sähen Zweifel an der Glaubwürdigkeit feindlicher Regierungen, diffamieren politische Gegner und tragen aktiv zur Polarisierung der Gesellschaften in westlichen Demokratien bei.[18] Interessanterweise geht es dabei nicht vorrangig um Russland oder Inhalte, die Russland direkt oder indirekt betreffen. Vielmehr zielen die Propagandakampagnen, die im Englischen treffender als *information warfare* bezeichnet werden, darauf, gesellschaftlichen Unfrieden zu stiften, politisches Chaos zu schüren und so die jeweilige Nation von innen heraus systematisch zu schwächen. Die hierfür notwendigen Mittel sind so einfach wie effektiv: Mithilfe einiger Hundert Mitarbeiter, falscher Social-Media-Accounts sowie Troll-Armeen und Bots gelang es etwa der Internet Research Agency aus Sankt Petersburg, zahlreiche gesellschaftliche Kontroversen anzuheizen, soziale Proteste anzuzetteln und in politische Wahlprozesse einzugreifen.[19] Wie weitreichend die Auswirkungen dieser technisch simplen digitalen Einflussnahme sein können, zeigte sich nicht zuletzt im US-Wahlkampf 2016, der von Russland aus mithilfe von Hackerangriffen und Social-Media-Kampagnen zugunsten des späteren Wahlsiegers und Präsidenten Donald Trump manipuliert wurde, wie der Bericht des Sonderermittlers Robert Mueller eindrücklich nachzeichnet.[20] Zahlreiche nachgewiesene russische Manipulationsversuche – vom Unabhängigkeitsreferendum in Katalonien (2017) über das Brexit-Referendum (2016) bis hin zur internationalen Berichterstattung über den russischen Oppositionspolitiker Alexei Nawalny – komplettieren das Bild einer fast omnipräsenten

Cybermacht, die sich subversiv in zahlreiche politische Debatten und Abstimmungsprozesse in anderen Staaten einmischt.

Venezuela

Ein weitaus weniger bekannter Akteur in der digitalen Sphäre ist hingegen Venezuela. Das südamerikanische Land befindet sich seit mehreren Jahren in einer humanitären Krise. Nahrungsmittelknappheit, Hyperinflation und extreme Armut plagen die Bevölkerung und haben seit 2018 fast ein Fünftel der venezolanischen Bevölkerung dazu veranlasst, den desolaten Umständen zu entfliehen. Doch das Land, das weder seine Bevölkerung ernähren kann noch dazu in der Lage ist, seine Strom- und Wasserversorgung zuverlässig aufrechtzuerhalten, ist

Gegensätze: Obwohl die venezolanische Regierung nicht einmal die Grundversorgung der eigenen Bevölkerung gewährleisten kann, spielt sie in Sachen Desinformation in der ersten Liga. Quelle: © Manaure Quintero, Reuters.

ein ernstzunehmender Spieler auf dem Feld der digitalen Subversion. Nicht von ungefähr zählt das Global Inventory of Organised Social Media Manipulation der Universität Oxford den südamerikanischen Staat im Jahr 2019 zur kleinen Führungsriege der globalen Manipulateure, die über eine hohe Cybertruppen-Kapazität verfügen.[21]

Die venezolanische Trollarmee versucht, durch eine massive Streuung von Fake News die Informationshoheit des Regimes zu sichern.

Für viele überraschend hat Venezuela schon seit mehreren Jahren eine Cyberstrategie, die von internationalen Analysten insbesondere mit Blick auf die Verbreitung von Propaganda als sehr schlagkräftig eingeschätzt wird. Bereits seit 2010 verfolgte Venezuela unter Präsident Hugo Chávez eine Strategie der aktiven Nutzung sozialer Netzwerke zur Verbreitung seiner politischen Botschaften und Mobilisierung seiner Anhängerschaft. Ab spätestens 2017 begann das südamerikanische Land mit dem Aufbau einer digitalen Armee, um sich im Cyberspace für den Informationskrieg zu wappnen, wie ein geleaktes Dokument des venezolanischen Innenministeriums mit dem Titel „Projekt zur Schaffung einer Trollarmee der bolivarianischen Revolution“ zeigt.[22]

Experten zufolge hat die venezolanische Trollarmee eine Stärke von mindestens 500 Personen, die – ergänzt durch digitale Bots – soziale Netzwerke wie YouTube, Facebook, Instagram, Telegram, WhatsApp und insbesondere Twitter belagern und durch die Verbreitung politischer Botschaften, Störungen der Social-Media-Kommunikation der demokratischen Opposition sowie die massive Streuung von Fake News die Informationshoheit des venezolanischen Regimes zu sichern versuchen.[23] Die „Desinformations-Einheiten“ der venezolanischen Cyberarmee sind in einer militärischen Struktur organisiert, wobei jede einzelne Einheit über 1.000 Social-Media-Accounts bedient. In Hochzeiten des Informationskampfes, wie den sozialen Protesten gegen den Nachfolger von Hugo Chávez, Nicolás Maduro, oder dem Beschluss der USA zur Verhängung internationaler Sanktionen gegen Venezuela im Jahr 2019, wurden Untersuchungen zufolge zwar über 80 Prozent des pro-chavistischen Social-Media-Traffics durch automatisierte Bots erzeugt. Im Unterschied zu anderen Staaten, die die sozialen Netzwerke zu Propagandazwecken manipulieren, sind in Venezuela jedoch vergleichsweise viele Trolle aus Fleisch und Blut am Werk.[24] Diese werden unter anderem mit Lebensmittelgutscheinen entlohnt, die angesichts der herrschenden Nahrungsmittelknappheit in dem krisengeplagten Land für viele wertvoller als eine monetäre Lohnzahlung in der hyperinflationären Landeswährung sind.

Mit seinen Cyberaktivitäten ist das südamerikanische Land nicht nur national, sondern auch international sehr aktiv. Dem Atlantic Council zufolge ist Venezuela das erste Land in Lateinamerika, das mithilfe von Cybertechnologie strategische Propaganda betreibt – und dies nicht nur im nationalen Rahmen.[25] Wie eine vergleichende Studie der Universität Oxford zeigt, zählt das wirtschaftlich verarmte Land sogar zur weltweiten Führungsriege von Staaten, die die Kapazitäten für Informationskampagnen mit globaler Reichweite aufweisen.[26] Dass Venezuela diese Kapazität durchaus erfolgreich zur Einflussnahme in anderen Staaten nutzt, zeigte sich in den letzten Jahren mehrfach. So mischte Venezuela sich, teilweise im Verbund mit Russland, mithilfe von künstlichen Social-Media-Konten und automatisierten Weiterverbreitungsinstrumenten in verschiedenste gesellschaftspolitische Kontroversen in Lateinamerika, aber auch z. B. in Spanien ein und schürte nachweislich gesellschaftliche Konflikte sowie eine Radikalisierung der entstehenden Protestbewegungen.[27] Nicht zufällig waren dabei ebenjene Staaten Ziel der subversiven venezolanischen Desinformationskampagnen, die sich zuvor international gegen das Maduro-Regime positioniert hatten.[28] Zwar wäre es vermessen, die unterschiedlichen gesellschaftlichen Konflikte in Chile, Ecuador und Kolumbien, die sich wie ein Lauffeuer ausbreiteten und im Herbst

2019 auf die ganze Region überzugreifen schienen, auf das Wirken Venezuelas zurückzuführen, doch die erfolgreichen Einmischungskampagnen demonstrierten eindrücklich das Potenzial zur Machtprojektion, das digitale Technologien bieten – insbesondere für Staaten ohne klassische Machtressourcen wie Venezuela.

Iran hat sich vom frühen Cyberopfer zu einer offensiv auftretenden Cybermacht entwickelt.

Iran

Auch die Islamische Republik Iran verfügt über Cyberkapazitäten und hat diese schon frühzeitig entwickelt. Vor dem Hintergrund der schmerzhaften Erfahrungen der Social-Media-Kampagnen der grünen Revolution von 2009, die das Regime stark unter Druck brachten, sowie des verheerenden Cyberangriffs auf iranische Atomanreicherungsanlagen in Form des Computerwurms Stuxnet im Jahr 2010 gründete der iranische Revolutionsführer Ali Chamenei zu Beginn des Jahres 2012 den Obersten Rat für Cyberspace. Als Gremium, das über alle cyberpolitischen Fragen entscheidet, befasst sich der Rat seit seiner Gründung nicht nur mit der Zensur unliebsamer Webinhalte, sondern auch mit der Abwehr der (relativ häufig stattfindenden) Cyberangriffe auf Iran sowie mit der aktiven Entwicklung eigener Kapazitäten zur Durchführung von Cyberattacken auf gegnerische Staaten. In Ermangelung klassischer militärischer Machtressourcen und unter dem Eindruck wirtschaftlicher Isolierung durch strenge internationale Sanktionen sieht Iran die Entwicklung und Nutzung digitaler Technologien als Möglichkeit, asymmetrische Kapazitäten der Kriegsführung zu erlangen und sein Potenzial zur Machtprojektion auf diese Weise beträchtlich zu steigern.

Zwar reichen die Cyberkapazitäten Irans nicht an diejenigen Russlands, der USA oder Israels heran, doch die Islamische Republik hat in den letzten Jahren große Fortschritte gemacht und sich vom frühen Cyberopfer zu einer offensiv auftretenden Cybermacht entwickelt, die in der Lage ist, auch technisch überlegenen Mächten empfindliche Verluste zuzufügen.[29] Die Angriffe richten sich dabei bewusst nicht gegen staatliche oder militärische Institutionen, sondern zielen auf privatwirtschaftliche Unternehmen in verfeindeten Staaten ab. So gelang es Iran beispielsweise 2012, durch DDoS-Angriffe auf mehr als ein Dutzend US-amerikanischer Großbanken einen enormen finanziellen Schaden anzurichten, der einzelne Banken zwang, mehrstellige Millionenbeträge in den Schutz vor weiteren iranischen Hackerangriffen zu investieren. Auch an der Wall Street konnte eine Iran nahestehende Hackergruppe 2013 – zumindest zeitweise – beträchtlichen Schaden anrichten, indem es gelang, das Twitter-Konto der Nachrichtenagentur Associated Press zu hacken und so Fake News über Explosionen im Weißen Haus und vermeintliche Verletzungen des US-Präsidenten zu verbreiten. Bis die Falschnachrichten ausgeräumt werden konnten, waren der Dow Jones um 150 Punkte gefallen und ca. 136 Milliarden US-Dollar vernichtet worden.[30]

Neben technisch simplen Hackerattacken mit beträchtlichen finanziellen Folgen für die Opfer gehören auch Desinformationskampagnen zum Repertoire iranischer Cyberkapazitäten. Insbesondere in der arabischen Welt ringt Iran um Einfluss in den sozialen Netzwerken und versucht mithilfe konzertierter Propagandakampagnen seinen Rivalen Saudi-Arabien zu schwächen. Hierbei werden gewöhnliche, computergestützte Social-Media-Kampagnen durch die aufwendige Imitation arabischer Nachrichtenseiten ergänzt, die das iranische Narrativ sowie Saudi-Arabien-kritische Inhalte in der Region verbreiten.[31]

Als internationaler Pariah-Staat ohne nennenswerte traditionelle Machtressourcen hat sich Iran somit in weniger als einer Dekade zu einer Cybermacht entwickelt, die zwar nicht in der allerersten Liga der *Cyber Superpowers* mitspielt, aber auf dem Gebiet der Cyberkriegsführung ein durchaus ernstzunehmender Akteur ist und ihre Regionalmachtambitionen gekonnt im digitalen Raum verfolgt.

Fazit

So unterschiedlich die oben erwähnten Fallbeispiele der kleineren und größeren Cybermächte sind, so klar ist die generelle Entwicklung, die sich abzeichnet: Digitale Fähigkeiten gewinnen zunehmend an Bedeutung in der internationalen Politik. Staaten, die in der Lage sind, Cyberoperationen durchzuführen, verzeichnen einen spürbaren Machtgewinn – Staaten, die diese Fähigkeiten nicht entwickeln, büßen an Gestaltungsspielraum in den internationalen Beziehungen ein.

Interessanterweise sind hierbei klassische Machtressourcen, wie militärische Stärke und Wirtschaftskraft, keine notwendige Voraussetzung für den Erfolg im digitalen Raum. Zwar zählt die erste Liga der Cybermächte auch viele traditionelle Großmächte in ihren Rängen. Doch um digitale Fähigkeiten zu entwickeln und als Machtressource auszuschöpfen, benötigt ein Staat nicht viel, wie die Beispiele der internationalen Außenseiter Iran und Venezuela zeigen. In gewisser Weise scheinen sich Cyberkapazitäten sogar in besonderer Weise zum Machtgewinn kleiner und mittelgroßer Staaten zu eignen, denn sie stellen ein schlagkräftiges Mittel zur asymmetrischen Kriegsführung dar. Trotz eines relativ geringen Ressourceneinsatzes und eines niedrigschwelligen technischen Entwicklungsniveaus besitzen digitale Technologien im Einsatz gegen andere Staaten das Potenzial, erheblichen Schaden anzurichten. Angriffe auf schlecht geschützte Behörden, Unternehmen oder auch Infrastruktur in gegnerischen Staaten können diese empfindlich treffen.

Da die Attribution in der Regel schwierig und oft erst mit erheblichem Zeitverzug möglich ist, bleibt das Risiko für den Angreifer kalkulierbar gering. Hinzu kommt, dass die Beweisführung selten eindeutig und das konsequente Abstreiten der Beteiligung Teil der Kriegsführung im Cyberspace ist.[32] Dies stellt auch einen der wesentlichen Unterschiede zu den bisherigen Machtkämpfen auf internationaler Ebene dar. Denn während der globale Wettbewerb um Bedeutung und Einfluss stets mit sichtbaren Machtdemonstrationen und dem Sammeln von Statussymbolen einherging, spielt sich der Wettkampf im Cyberspace im Unsichtbaren ab.

Durch informationelle Kriegsführung erlangen Staaten international Einfluss, die bislang nicht als globale Akteure galten.

Dies macht eine Anerkennung der gegenwärtig stattfindenden Machtverschiebungen besonders schwierig. Insbesondere auf dem Feld der informationellen Kriegsführung, einem Bereich mit wachsender Bedeutung in nationalen, aber auch internationalen Konflikten, erlangen Staaten international Einfluss, die die Weltgemeinschaft bislang nicht als globale Akteure auf dem Radar hatte. Diese Staaten haben jedoch das Machtpotenzial, das ihnen digitale Technologien bieten, früh erkannt und schöpfen es bereits erfolgreich aus. Viele von ihnen haben durch die Anwendung von Techniken der informationellen Kriegsführung gegen ihre eigene Bevölkerung und Opposition jahrelange Erfahrung auf diesem Gebiet und wenden ihr Know-how nun auch im internationalen Rahmen an, um sich global Einfluss zu verschaffen.

Staatlichen Stellen in Deutschland ist diese Gefahr bekannt, wie die Cyberkapitel der jährlichen Verfassungsschutzberichte und die bereits im Jahr 2011 erfolgte Schaffung des Nationalen Cyber-Abwehrzentrums (Cyber-AZ) dokumentieren. Doch in der breiteren Bevölkerung gibt es bislang wenig Bewusstsein für die subversiven Cyberaktivitäten fremder Staaten, die eben nicht nur auf die Spionage von Regierung und Wirtschaft abzielen, sondern über Desinformationskampagnen die Manipulation der öffentlichen Meinung – und damit die Bevölkerung selbst – ins Visier nehmen. Hier bedarf es breit angelegter Aufklärungskampagnen, die konkrete Beeinflussungsversuche ausländischer Staaten publik machen und Bürgerinnen und Bürger aktiv für

diese subtile Art der externen Einflussnahme sensibilisieren. Nur wenn Angriffsflächen und Gefahrenpotenziale von Cyberangriffen der breiten Bevölkerung bekannt sind, kann vermieden werden, dass Deutschland zur cyberpolitischen Zielscheibe wird.

Jason Chumtong ist Referent für Künstliche Intelligenz der Konrad-Adenauer-Stiftung.

Dr. Christina Stolte ist Referentin für die Anden-länder, das Rechtsstaatsprogramm Lateinamerika sowie das Regionalprogramm Politische Partizipation Indigener der Konrad-Adenauer-Stiftung.

1 Dargin, Justin 2013: The Rise of the Global South, Philosophical, Geopolitical and Economic Trends of the 21st Century, Singapur.
2 Kello, Lucas 2017: The Virtual Weapon and International Order, New Haven.
3 Macht wird hier definiert nach Max Weber als „jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht". Weber, Max 1972: Wirtschaft und Gesellschaft: Grundriß der verstehenden Soziologie, 5. Auflage, Tübingen, S.28. Klassische Machtressourcen im zwischenstaatlichen Machtstreben umfassen militärische Fähigkeiten (Größe der Armee, verfügbare Waffen und technisch-logistische Ausstattung des Militärs) sowie die Wirtschaftskraft eines Staates (BIP, Wohlstand und wirtschaftlicher Entwicklungsgrad).
4 Rosenbach, Eric 2020: A Note to Readers, in: Voo, Julia / Hemani, Irfan / Jones, Simon / DeSombre, Winnona / Cassidy, Dan / Schwarzenbach, Anina (Hrsg.): National Cyber Power Index 2020. Methodology and Analytical Considerations, Belfer Center for Science and International Affairs, 09/2020, S.iv, in: https://bit.ly/37MeWLO [25.02.2021].
5 Prier, Jarred 2017. Commanding the Trend: Social Media as Information Warfare, in: Strategic Studies Quarterly 11: 4, S.50–85, in: https://bit.ly/3r3N2Tf [02.03.2021]; Harknett, Richard J. / Smeets, Max 2020: Cyber campaigns and strategic outcomes, Journal of Strategic Studies, 04.03.2020, in: https://bit.ly/3bSnoum [02.03.2021].
6 Voo et al. 2020, N. 4.
7 Kahn, Herman 2010: On Escalation. Metaphors and Scenarios, London.
8 Kostyuk, Nadiya / Powell, Scott / Skach, Matt 2018: Determinants of the Cyber Escalation Ladder, in: The Cyber Defense Review 3: 1, S.123–134, in: https://bit.ly/3sGDY77 [02.03.2021].
9 Baezner, Marie / Robin Patrice 2017: Hotspot Analysis: Stuxnet, Center for Security Studies (CSS), 10/2017, in: https://bit.ly/3aShhqz [13.01.2021].
10 Borghard, Erica D. / Lonergan Shawn W. 2019: Cyber Operations as Imperfect Tools of Escalation, in: Strategic Studies Quarterly, 13: 3, S.128 ff., in: https://jstor.org/stable/26760131 [02.03.2021].
11 Inglis Chris 2018: Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace, in: Lin, Herbert / Zegart, Amy (Hrsg.): Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations, Washington, S.19–44, hier S.25.
12 Eliason, William T. 2019: An Interview with Paul M. Nakasone, in: Joint Force Quarterly 92, S.7 f., in: https://bit.ly/3qXAhcI [13.01.2021].
13 Wiggen, Johannes 2020: Im Zustand des Unfriedens. Staatliche Cyberoperationen unterhalb der Schwelle bewaffneter Konflikte, Die Politische Meinung 565, Konrad-Adenauer-Stiftung, S.24–29, in: https://bit.ly/3b5tqsq [02.03.2021].

14 Schulze, Matthias 2021: 23 WTF ist Cyber Eskalation? Eskaliert der Hackback?, Perception, Podcast, 01.01.2021, in: https://bit.ly/2ZOy47D [25.02.2021].
15 International Committee of the Red Cross 2010: Cyber warfare, 29.10.2010, in: https://bit.ly/3r9TLv5 [02.03.2021].
16 Akimenko, Valeriy / Giles, Keir 2020: Russia's Cyber and Information Warfare, Asia Policy 15: 2, S. 67–75, 29.04.2020, in: https://bit.ly/3kAq0B7 [02.03.2021].
17 Voo, Julia / Hemani, Irfan / Jones, Simon / DeSombre, Winnona / Cassidy, Dan / Schwarzenbach, Anina 2020: Reconceptualizing Cyber Power. Cyber Power Index Primer, Report der China Cyber Policy Initiative, 04/2020, in: https://bit.ly/302wwap [25.02.2021].
18 Buchanan, Ben 2020: The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics, Cambridge.
19 Chen, Adrian 2015: The Agency, The New York Times Magazine, 02.06.2015, in: https://nyti.ms/3bDJQan [25.02.2021]; Kosoff, Maya 2017: How Russia Secretly Orchestrated Dozens of U.S. Protests, Vanity Fair, 30.10.2017, in: https://bit.ly/3dLVwe4 [25.02.2021].
20 Mueller, Robert S. 2019: Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, 03/2019, in: https://bit.ly/3dLCvIs [25.02.2021].
21 Bradshaw, Samantha / Howard, Philip N. 2019: The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation, Working Paper 2, Project on Computational Propaganda, in: https://bit.ly/37Na9tz [25.02.2021].
22 Ministerio de Interior, Justicia y Paz 2017: Proyecto de Formación del Ejército de Trolls de la Revolución Bolivariana, in: https://bloom.bg/3pQAcpX [25.02.2021].
23 Transparencia Venezuela 2019: La desinformación, estrategia intencional del Poder, Informe de Corrupción, in: https://bit.ly/3bHp5KS [25.02.2021].
24 Bradshaw, Samantha / Howard, Philip N. 2019, Case Studies – Collated, 11/2019, Venezuela, S. 126–128, in: https://bit.ly/3knD7VV [02.03.2021].
25 Suárez Pérez, Daniel / Ponce de Leon Rosas, Esteban 2021: Digital Autocrazy. Maduro's control of the Venezuelan information environment, Atlantic Council, 03/2021, in: https://bit.ly/3uP6DYR [14.04.2021].
26 Bradshaw / Howard 2019, N. 21.
27 Coscojuela, Saraí / Quintero, Luisa 2019: Tropa virtual de Maduro bombardea las redes para desinformar, RunRunEs, 28.11.2019, in: https://bit.ly/3qUa1jC [25.02.2021].
28 Organization of American States (OAS) 2019: Statement of the OAS General Secretariat, Pressemitteilung, 16.10.2019, in: https://bit.ly/3sqhYNJ [25.02.2021].
29 Slavin, Barbara / Healey, Jason 2013: Iran: How a Third Tier Cyber Power Can Still Threaten the United States, Atlantic Council Issue Brief, 29.08.2013, in: https://bit.ly/37Onr9f [25.02.2021].
30 Gross, Michael Joseph 2013: Silent War, Vanity Fair, 07/2013, in: https://bit.ly/2ZRVby2 [06.01.2021].
31 Elswah, Mona / Howard, Philip N. / Narayanan, Vidya 2019: Iranian Digital Interference in the Arab World, COMPROP Data Memo, 03.04.2019, in: https://bit.ly/3pMIbEA [25.02.2021].
32 Carson, Austin 2019: Secret Wars. Covert Conflict in International Relations, Princeton; Hofstetter, Yvonne 2019: Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, München.