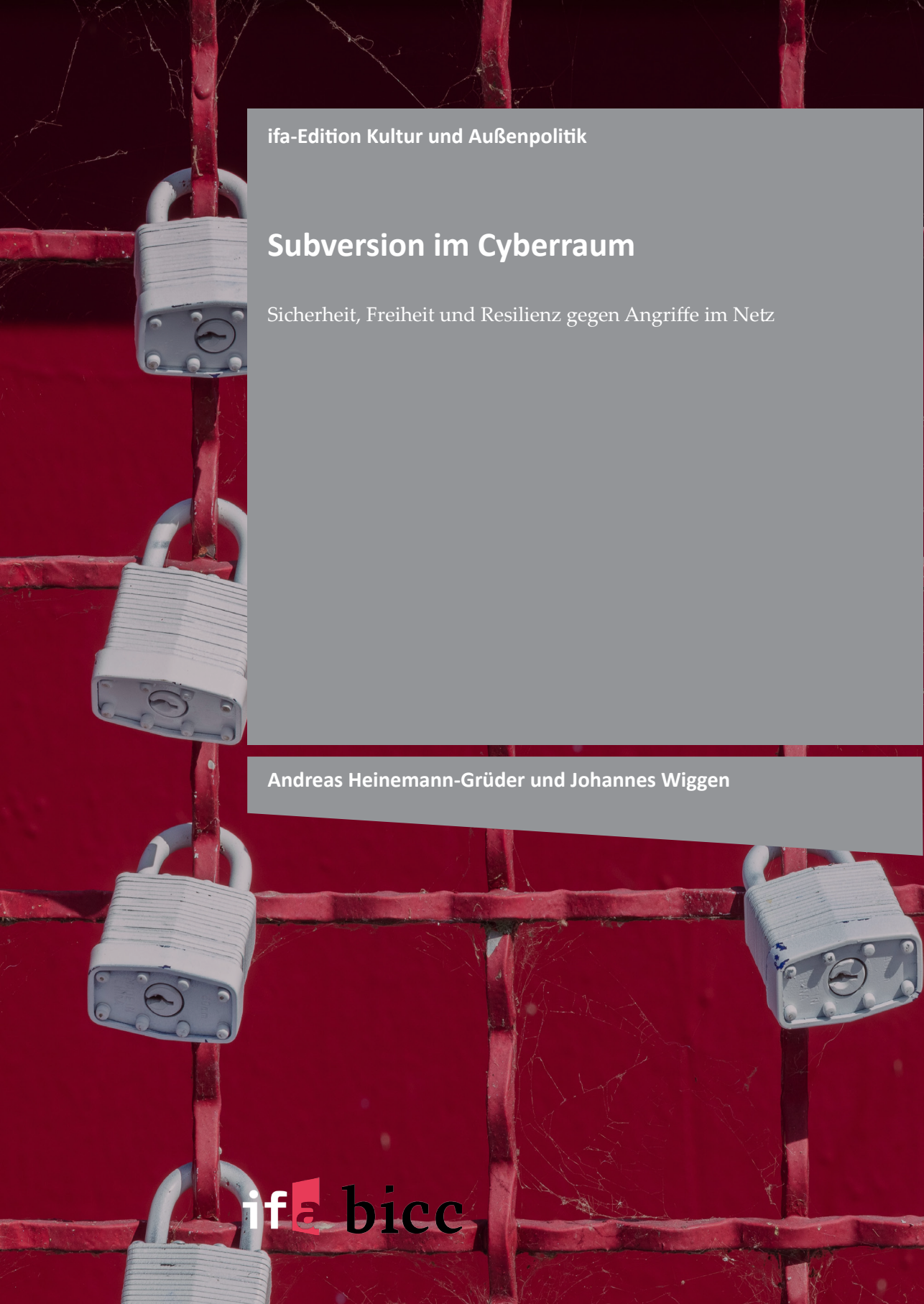
Subversion im Cyberraum: Sicherheit, Freiheit und Resilienz gegen Angriffe im Netz

Heinemann-Grüder, Andreas; Wiggen, Johannes

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Empfohlene Zitierung / Suggested Citation:
Heinemann-Grüder, A., & Wiggen, J. (2020). *Subversion im Cyberraum: Sicherheit, Freiheit und Resilienz gegen Angriffe im Netz.* (ifa-Edition Kultur und Außenpolitik). Stuttgart: ifa (Institut für Auslandsbeziehungen). https://doi.org/10.17901/AKBP1.01.2020



ifa-Edition Kultur und Außenpolitik

Subversion im Cyberraum

Sicherheit, Freiheit und Resilienz gegen Angriffe im Netz

Andreas Heinemann-Grüder und Johannes Wiggen

ifa bicc

ifa-Edition Kultur und Außenpolitik

Subversion im Cyberraum

Sicherheit, Freiheit und Resilienz gegen Angriffe im Netz

Andreas Heinemann-Grüder, Johannes Wiggen

ifa Institut für Auslandsbeziehungen

bicc Bonn International Center for Conversion

Inhaltsverzeichnis

Vorwort

Der schmale Grat zwischen Sicherheit und Freiheit befindet sich in einem ständigen Prozess neuer Aushandlung. Dies ist vor allem der Fall, wenn sich ökologische, gesellschaftliche, ökonomische oder technische Rahmenbedingungen rasant verändern und hierdurch neue Bedrohungen und Risiken auftreten. So hat die digitale Revolution gesellschaftliche, wirtschaftliche und politische Prozesse globalisiert und Interaktionsformen drastisch verändert. Hierdurch wurden neue Möglichkeiten, aber auch Unabwägbarkeiten hervorgerufen. In der digitalen Kommunikation entstand vor allem Unsicherheit darüber, in welcher Weise Wahrnehmungs- und Kontrollmöglichkeiten eingeschränkt, manipuliert und verändert werden. Denn zum einen ist die Kommunikation im Cyberraum oftmals nicht transparent und eindeutig; zum anderen geht die Deutungshoheit der Medien zur Meinungsbildung sowie ihre politische Kontrollfunktion durch die Pluralisierung der Informationsangebote verloren. Populisten, Fake News und Desinformationen gewinnen in diesem Umfeld schnell an Einfluss. Hierdurch veränderten sich nicht nur im privaten, sondern auch im öffentlichen und medialen Raum Interaktion. Wie hoch der Vertrauensverlust in die digitale Kommunikation sein wird, ist gegenwärtig noch nicht abzuschätzen. Vor diesem Hintergrund tritt die Notwendigkeit deutlich zutage, dass Regierungen, Zivilgesellschaft und Wirtschaft vor der Herausforderung stehen, neue Verbindlichkeiten und Regeln zu schaffen.

Zusätzlich zu dieser grundlegenden Verunsicherung in der digitalen Kommunikation nehmen bewusst gesetzte Bedrohungen und Gefahren im Cyberraum durch Angriffe staatlicher und nicht-staatlicher Akteure stetig zu. Dies wiederum führt zu einer weltweiten Verstärkung der Sicherheitsdiskurse bezogen auf den Cyberraum und einem damit einhergehenden digitalen Wettrüsten. Um jedoch auf den neuen „Kalten Krieg" im Cyberraum richtig reagieren zu können, ist es wichtig, über zentrale Begrifflichkeiten ein gemeinsames Verständnis zu gewinnen, konkurrierende Diskurse miteinander in Beziehung zu setzen und hieraus resultierende Handlungsszenarien zu untersuchen. Wie kann Vertrauen im Cyberraum geschaffen werden? Wie kann in der Cyberwelt die Balance zwischen dem Wunsch nach individuellen Freiheiten und nach kollektiven Sicherheitsinteressen austariert werden? Was bedeuten verschiedene Verständnisse und Veränderungen des Sicherheitsbegriffs für internationale und multilaterale Zusammenarbeit? Was kann internationale Kulturarbeit leisten, um digitale Freiräume zu definieren sowie Normen und Werte im Cyberraum zu verankern? Diesen Fragen widmen sich die beiden Autoren der vorliegenden Studie, Andreas Heinemann-Grüder und Johannes Wiggen. Die Autoren analysieren aktuelle Sicherheitsbedrohungen im Cyberraum, v. a. Subversion, untersuchen Sicherheitsdiskurse im internationalen Vergleich und zeigen Möglichkei-

ten auf, wie individuelle Freiheiten und kollektive Sicherheitsinteressen miteinander in Einklang gebracht werden können.

Die Studie greift auch die Ergebnisse eines gemeinsam von BICC und ifa organisierten Workshops auf, der am 23. Mai 2019 am BICC in Bonn stattfand. Wir möchten in diesem Zuge nicht nur den beiden Autoren dieser Studie herzlich für ihre Arbeit danken, sondern auch den Teilnehmenden des Workshops für ihre wichtigen Impulse. Dieses Forschungsprojekt wurde im Rahmen des ifa-Forschungsprogramms „Kultur und Außenpolitik" in Kooperation mit BICC umgesetzt. Wir möchten auch unseren Kolleginnen danken, die das Projekt konzeptionell und organisatorisch unterstützten: Susanne Heinke (BICC), Odila Triebel (ifa), Sarah Widmaier (ifa) und Anja Schön (ifa).

Der Umgang mit der Digitalisierung unserer Lebenswelten ist eine politische und gesellschaftliche Gestaltungsaufgabe. Um Sicherheit im Netz zu erreichen, sollten gemeinsam aufgestellte Regeln von Regierungen, transnationalen Organisationen, Zivilgesellschaft und der Industrie befolgt werden. Der von Emmanuel Macron initiierte *Paris Call for Trust and Security in Cyberspace* ist hierzu ein bedeutender Schritt. Vertrauensbildende Maßnahmen sind u. a. das Teilen von Informationen, internationale Kooperationen, der Aufbau gemeinsamer Abwehr-Kapazitäten sowie die verstärkte Investition in die Entwicklung von sicheren Technologien. Zum Anstoß solcher Prozesse müssen divergierende Perspektiven zusammengebracht und verstanden werden. Hierzu soll die vorliegende Studie einen Beitrag leisten.

Ronald Grätz
Generalsekretär
ifa (Institut für Auslandsbeziehungen)

Prof. Dr. Conrad Schetter
Director for Research
Bonn International Center
for Conversion (BICC)

Zusammenfassung

Die technischen Möglichkeiten der Cyberwelt haben gänzlich neue Potenziale zur Beeinflussung von politischen Präferenzen in anderen Staaten eröffnet. Die Meinungsbildung in offenen Gesellschaften wird zunehmend durch subversive Maßnahmen autoritärer Regime im Internet beeinflusst, wodurch der öffentliche Raum Internet stark eingeschränkt wird. In dieser Studie wird untersucht, wie die Resilienz von offenen Gesellschaften gegen Subversion aus dem Cyberraum gestärkt werden kann, ohne dabei die eigenen Grundsätze preiszugeben. Zunächst wird ein Überblick zu den Diskursen über Cyberbedrohungen gegeben, um sich dann auf die Frage nach der gesellschaftlichen Resilienz zu konzentrieren.

1. Cyberangriffe im Spannungsfeld von Freiheit und Sicherheit

Autoritäre bzw. nicht-demokratische Staaten wie Russland, China, der Iran, Nordkorea oder die Türkei beeinflussen durch das Internet, durch traditionelle Massenmedien und soziale Medien sowie durch Einflussagenten die Meinungsbildung und das Wahlgeschehen in offenen Gesellschaften. Die neue Systemauseinandersetzung findet innerhalb und zwischen Gesellschaften mit unterschiedlicher politischer Ordnung statt. Im Unterschied zum Kalten Krieg ist „der Westen" allerdings in sich gespalten. Autoritäre Regime sind wiederum nicht hermetisch abgeschlossen.

Gibt es eine gemeinsame Grundlage, auf die sich unterschiedliche politische Regime verständigen könnten, d.h. Sicherheitsnormen und Normen, die den Schutz des öffentlichen Raums Internet betreffen? Nicht zuletzt die Auswärtige Kulturpolitik muss sich unter den Bedingungen des Cyberraumes – den Möglichkeiten und Gefährdungen – fragen, wie und mit welchen Mitteln sie zu einer freien, friedlichen und sicheren Welt beitragen und für ihre Werte und Normen einstehen kann.

Die technischen Möglichkeiten der Cyberwelt haben gänzlich neue Potenziale für die Eroberung von Köpfen und Herzen und die Beeinflussung von politischen Präferenzen in anderen Staaten eröffnet. Während des Ost-West-Konflikts firmierte die Einflussnahme sozialistischer Staaten als „Agitation und Propaganda" und war meist leicht zu durchschauen; „der Westen" fühlte sich – bis auf gelegentliche Phasen systemkritischer Mobilisierung – normativ und argumentativ dem „Osten" weit überlegen: Die Attraktivität des westlichen Systems war für die Bürger „im Osten" weitaus höher als umgekehrt.

Die folgende Studie fragt, wie die Resilienz von offenen Gesellschaften gegen Subversion aus dem Cyberraum gestärkt werden kann, ohne dabei die eigenen Grundsätze preiszugeben. Zunächst wird ein Überblick zu den Diskursen über Cyberbedrohungen gegeben, um sich dann auf die Frage nach der Resilienz zu konzentrieren.

„Cyberraum", „Cyberspace" oder „Cyberdomäne" sind weit gefasste, amorphe Begriffe, mit denen die soziale, interaktive und technische Dimension von digitalen Netzwerken, Systemen und Geräten beschrieben wird. Cyberangriffe firmieren wiederum unter drei Begriffen: Sabotage, Spionage und Subversion. Cyberangriffe können von Staaten und von nicht-staatlichen Akteuren lanciert werden, die Grenzen sind aufgrund des Attributionsproblems fließend. Gleichwohl agieren Staaten als direkte oder indirekte Auftraggeber bzw. als Operateure von Cyberangriffen und bedrohen so die Sicherheit und Integrität anderer Staaten. Verwundbarkeiten und Angriffspotenziale beziehen sich

auf die interaktiv-kommunikative und auf die technische Dimension. Die Felder überschneiden und beeinflussen sich. Spionage und Sabotage zielen auf die illegale Beschaffung von sensiblen Informationen und auf die Integrität kritischer Infrastrukturen. Sabotage meint Angriffe auf technische Systeme wie Kraftwerke, Stromnetze oder Kontrollsysteme. Spionage wiederum erstreckt sich auf die Wirtschaft, militärische Geheimnisse, nicht autorisierten Datenerwerb und die geheimdienstliche Zusammenarbeit. Subversion schließlich bezieht sich auf die politische Mobilisierung über soziale Netzwerke, die Verbreitung von Falschnachrichten oder die Manipulation von Wahlen und sucht die ideellen bzw. normativen Grundlagen gegnerischer Gesellschaften zu untergraben.

Die vorliegende Studie konzentriert sich auf eine Form der Nutzung des Cyberraumes, nämlich auf die manipulative bzw. subversive Einflussnahme auf die politische Willensbildung (Löwenstein 1937a und 1937b; Mannheim 1943). Offene, liberale Gesellschaften werden nicht nur von außen infrage gestellt, sondern zunehmend von innen. Nationalismus, Protektionismus, die Ablehnung von Multiethnizität und liberalen Werten durchziehen drei Jahrzehnte nach dem Ende des Ost-West-Konflikts auch die hiesigen Gesellschaften. Mit welchen Mitteln sollen und können sich offene Gesellschaften gegen Angriffe auf ihren normativen Kernbestand erwehren?

Demokratien sind für Subversion anfälliger als autoritäre Regime, weil die Kontrollmöglichkeiten des Staates rechtlichen Beschränkungen unterliegen. Doch wie sollte die Resilienz dann gestärkt werden, ohne die Demokratie selbst zu beschädigen (Hagmann 2012; Malkki/Teemu 2016)? Wie wehrhaft darf Demokratie sein, ohne die Ergebnisoffenheit von Diskursen und Wahlen selbst anzugreifen? Gilt Resilienz wechselseitig, weil Demokratien, z.B. die USA, ihrerseits versuchen, die Öffentlichkeit in autoritären Staaten über soziale Medien oder das Internet zu erreichen? Die Digitalisierung und Vernetzung der Welt bestimmen zunehmend das internationale Denken und Handeln, die Kommunikation globalisiert sich, kaum ein Regime kann die Hegemonie der eigenen Wertegemeinschaft ohne fundamentale Herausforderungen behaupten. Der Cyberraum bietet Chancen für Austausch und Interdependenz, es kollidieren aber zugleich unterschiedliche Werte und Rechtsvorstellungen.

1.1 Cyberwar: Realität oder Chimäre?

Sicherheitsstudien befassen sich seit Jahren mit den Folgen von Angriffen aus dem Cyberraum. Die einen sprechen von einer „Revolution“ in der Bedrohungslage und für die Sicherheitspolitik schlechthin (Clarke/Knake 2012; Kello 2013 und 2018), andere betonen Kontinuitäten zu alten Formen zwischenstaatlicher Konflikte, demnach entwickeln sich

Cyberbedrohungen evolutionär (Rid 2012; 2017; Gartzke 2013; Lindsay 2013). Der Grad an Alarmismus bei der Rede von Cyberbedrohungen ist von den Eigeninteressen des Sicherheitsestablishments, insbesondere der Geheimdienste, und den Enthüllungen durch Wikileaks und den Whistleblower Edward Snowden beeinflusst. Aufgrund der Risiken, Unwägbarkeiten, Verwundbarkeiten und möglichen Kontrollverlusten ziehen Vertreter des Sicherheitsestablishments oft Parallelen zum Krieg, daher die Rede vom Cyberwar. Je weiter die Redner vom Objekt der Bedrohung entfernt sind, umso schriller fallen gemeinhin die Kassandrarufe aus.[1] Die Grenze zwischen Krieg und Frieden, zwischen innerer und äußerer Sicherheit verwischt jedoch zusehends. Die vieldeutige Bestimmung des Begriffs „Cyberwar" illustriert dies: handelt es sich um eine Form des Krieges, um Spionage, um Diversion, um Sabotage, um Subversion, um Kriminalität oder schlicht die unregulierte Nutzung von verfügbaren Technologien? Die Ungewissheit darüber, welche Gefahren wirklich damit einhergehen, lässt Phantasien über unvorhersehbare Angriffe und Eskalationsdynamiken sprießen. Einige Autoren beschwören das klassische Sicherheitsdilemma herauf: Wer vom Schlimmsten beim Gegner ausgeht, wird sich selbst entsprechend offensiv und defensiv wappnen und damit selbst zur Eskalation im Sinne einer sich selbst erfüllenden Prophezeiung beitragen (Buchanan 2017: 114).

Bereits vor mehr als 25 Jahren erkannten US-Forscher die Bedeutung der Informations- und Kommunikationstechnologie für militärische Zwecke. John Arquilla und David Ronfeldt von der RAND-Corporation erklärten 1993 in dem Aufsatz *„Cyberwar is Coming!"*, dass die Informationsrevolution die Art und Weise verändern würde, wie Gesellschaften Konflikte austragen und Kriege geführt werden. Sie definierten „Cyberwar" als den militärischen Schutz der eigenen Kommunikations- und Informationssysteme bei gleichzeitiger Zerstörung bzw. Einschränkung der Funktionalität der Systeme des Gegners (Arquilla/Ronfeldt 1993: 26/30). Die strategische und taktische Nutzung von Information sollte militärische Ungleichgewichte kompensieren.

„Netwars" würden ein weites Repertoire der Kriegsführung mit geringer Intensität umfassen, nämlich die strategische Zusammenführung von diplomatischen Mitteln, Propaganda, psychologischen Kampagnen, politischer und kultureller Subversion, Täuschung oder Beeinflussung lokaler Medien, die Infiltration von Computer- und Datennetzwerken und die Förderung von Oppositionsgruppen mit dem Ziel der Beeinflussung

[1] vgl. Rid: *„But the wider one moves in political or military circles, in think tanks, parliaments, ministries, and military academics, the lower seems the density of genuine experts and the higher pitched the hyperbole*" (Rid 2017: ix).

der öffentlichen Meinung und der Eliten. „Netwars" sollten die Risiken und Kosten konventioneller Kriegsführung minimieren und das Repertoire der Durchsetzung des eigenen Willens erweitern.

Dass es sich bei Cyberangriffen um die neue Kriegsführung des 21. Jahrhunderts handelt, ist freilich umstritten. Entgegen der inflationären Rhetorik ist ein umfassender „Cyberwar" bisher ausgeblieben. Rid erklärte daraufhin schmissig: *„Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future"* (Rid 2012: 6). Als Krieg wird gemeinhin ein kollektives, organisiertes, mit Waffen ausgetragenes Verhalten bezeichnet, das tatsächlich oder potenziell tödliche, massive, kompakte Gewalt anwendet, um einen Gegner zur Erfüllung des eigenen – meist politischen – Willens zu zwingen. Mindestens einer der beteiligten Akteure ist nach der klassischen Kriegsdefinition ein Staat, zudem haben Kriegsstatistiker – recht willkürlich – mindestens tausend kriegsbedingte Tote pro Jahr zum Definitionsmerkmal erhoben. Danach ist ein Cyberkrieg in der Tat bestenfalls Zukunftsmusik.

Cyberangriffe können indes durch externe Mächte erfolgen und die Souveränität, Integrität und Infrastruktur eines Staates bzw. seiner Subjekte zum Ziel haben, die Schäden können auch ohne direkte Gewalteinwirkung massiv sein. Cyberangriffe können, müssen jedoch keine Kriegshandlungen darstellen. Bisher handelt es sich bei Cyberangriffen vorwiegend um asymmetrische Konflikte mit irregulären Gewaltakteuren, die – bezogen auf die Gewaltopfer – „niedrigschwellig" sind. Auch wenn es Präzedenzfälle wie Stuxnet, mit denen die USA und Israel zwischen 2009 und 2010 ca. 1.000 iranische Uranzentrifugen zerstörten (vgl. Lindsay 2013), oder die Cyberoperation gegen drei ukrainische Stromverteilungsstationen, die im Dezember 2015 in einen großflächigen, ein bis sechsstündigen Stromausfall resultierte (vgl. Zetter 2016), gibt: Physische Schäden sind bei Cyberangriffen bislang nicht das Primärziel, zudem sind staatliche Gewaltakteure nicht zwingend als Täter oder Auftraggeber ausgemacht.

Manche Beobachter sehen allerdings in Cyberattacken eine Fortführung der „*Revolution in Military Affairs*", die seit den 1970er Jahren von Militärtheoretikern ausgerufen worden war, und sich durch Informationsoperationen, die Nutzung des Weltraums, die Militarisierung ziviler Aktivitäten, die Anwendung von Daten als Waffe und eine vernetzte Operationsführung auszeichnete (Freedman 2013: 214 ff.). Die Nutzung des Cyberraums für Angriffe weist einige Besonderheiten auf: Sie ist billig, die Techniken sind auch von kleinen Staaten und nicht-staatlichen Akteuren anwendbar und leicht zugänglich – man könnte geradezu von der Demokratisierung des Krieges sprechen. Operationen können

zudem delegiert werden, z.B. durch Outsourcing an „patriotische Hacker". Nicht-staatliche Akteure agieren autonom – mit welchen Absichten auch immer – im Cyberspace, freilich verfügen Staaten nach wie vor über deutlich potentere Cyberfähigkeiten, um die nationale Sicherheit anderer Staaten zu beeinträchtigen.

Für kleinere Staaten und nicht-staatliche Akteure sind Sabotageoperationen, etwa das Löschen von Daten praktikable Optionen, darunter sogenannte Wiper-Operationen (z.B. NotPetya, Wannacry, Shamoon) oder die Blockade von Webseiten mit DDoS-Attacken (*Distributed-Denial-of-Service Attack,* z. B. Estland 2007). Kleinere Mächte können nicht mehr durch Großmächte in ihrem Verhalten gelenkt werden – ein Grund für die Panik unter den traditionellen Großmächten, die sich ihrer Ordnungsmacht beraubt sehen. Gleichwohl sind gezielte Sabotageoperationen, die physische Zerstörung oder Schädigung bewirken sollen, aufgrund der dazu nötigen Ressourcen, des Know-hows, der Angst vor Vergeltung, d.h. hoher politischer Kosten sowie der Notwendigkeit, unentdeckt bleiben zu müssen, um effektiv zu sein, bisher nur durch wenige potente Akteure durchführbar (Gartzke 2013; Lindsay 2013; Gartzke/Lindsay 2015; Valeriano/Maness 2015). Im Bereich der Sabotage kritischer Infrastruktur ist immer noch von der Mobilisierung staatlicher Ressourcen auszugehen.

Cyberangriffe werden vorwiegend von irregulären, d.h. rechtsstaatlich nicht autorisierten Akteuren oder Agenturen ausgeführt. Die Grenze zwischen militärischen und nicht-militärischen Zielen, zwischen Kombattanten und Nicht-Kombattanten verschwimmt, womit die Probleme direkter oder indirekter Attribution wachsen. Sabotageoperationen im Cyberraum, die in physische Effekte münden, können freilich durchaus die Schwelle eines bewaffneten internationalen Konflikts erreichen (Schmitt 2013: 75). Die Nutzung des Cyberspace für Angriffe dürfte insbesondere in Kriegszeiten qualitative Sprünge machen. Selbst ohne direkte Gewalteinwirkung verursachen Cyberangriffe massive ökonomische, politische und gesellschaftliche Schäden. Die Entwicklung von Cyber-Angriffskapazitäten wurde zunächst von den USA forciert und dann von anderen Ländern nachgeahmt.[2] Cyber-Angriffe können sich nicht nur gegen militärische Gegner, sondern auch gegen Bündnispartner richten.

In Demokratien stellt sich die Frage, ob Geheimdienste die Netze anderer Staaten „hacken", d.h. in diese eindringen dürfen. Was sind angemessene Normen des Verhaltens im

[2] vgl. dazu und zum folgenden Ruhmann (2012); https://www.wissenschaft-und-frieden.de/seite.php?artikelID=1822.

Cyberraum, darf jeder Staat tun, was zum Repertoire seines potenziellen Gegners gehört, nur um nicht in eine strukturell schwächere Position zu geraten? Cyberoperationen finden jedenfalls auch in Demokratien in einer normativen und rechtlichen Grauzone statt. In Demokratien ist der Modus operandi für staatliche Akteure im Cyberraum meist irregulär, d.h. sie operieren verdeckt. Je nach Land variiert auch die Einbindung von explizit irregulären Akteuren. In Russland werden Cyberkriminelle rekrutiert und – unter Druck – in staatliche Operationen inkorporiert; in China wiederum werden private Akteure schon in der Schule und an den Universitäten angeworben und institutionell integriert (Maurer 2018).

Bewertungen von Cyberattacken sind in hohem Maße von der Fähigkeit zur Attribution abhängig: Wer sind die Täter? Wer ist der Aggressor, wenn die Täter weit entfernt von den Orten, den Wirkungen und den Opfern von Gewaltakten operieren? Wie ernst, unmittelbar, direkt, invasiv und messbar ist ein Angriff und wie legitim sind Gegenreaktionen, z.B. die Ausweitung „militärischer Notwendigkeiten" auf Zivilisten oder auf zivile Fähigkeiten? Wie ließe sich begründen, dass militärische Reaktionen notwendig, verhältnismäßig und differenziert sind? Welche Art der Verteidigung gegen Cyberangriffe wäre legitim – passive oder aktive Verteidigung, offensive Verteidigung oder „nur" politische Reaktionen? Wer könnte militärische Verteidigung gegen Cyberangriffe autorisieren – der UN-Sicherheitsrat oder Staaten kraft ihres Rechtes auf Selbstverteidigung?

Die Fülle der Fragen belegt, dass die Rede vom „Cyberwar" von konzeptioneller Unklarheit durchzogen und von einer rechtlichen Grauzone umgeben ist. Am ehesten ließe sich noch der völkerrechtliche Bann von „unterschiedslosen Waffen" auf „Malware", auf „Logic Bombs" und auf militärische Angriffe auf die zivile Infrastruktur anwenden, ansonsten ist die Rede vom „Cyberwar" jedoch eher plakativer als analytischer Natur. Die Rede vom Krieg sollte deshalb auf Fälle massiver physischer Schädigung, insbesondere Tote, infolge von Gewalteinwirkung beschränkt bleiben.

Eine Präzisierung ist gleichwohl angezeigt: Ob ein Cyberkrieg stattfindet, wird mit einer gewissen Wahrscheinlichkeit nicht von den technischen Möglichkeiten diktiert, sondern dem Willen der Akteure: Wer sich auf einen Cyberkrieg rhetorisch, strategisch, taktisch und operativ vorbereitet, erhöht damit die Wahrscheinlichkeit, dass er tatsächlich stattfindet, zumindest solange das Abschreckungspotenzial, vergleichbar dem atomaren Terrorfrieden, nicht die Option der Selbstauslöschung einschließt. Umgekehrt gilt dann auch, ob ein Cyberkrieg nicht stattfindet, hängt von dessen normativer und kognitiver Einhegung und Delegitimierung ab.

Die Rede vom Cyberwar entgrenzt das Repertoire an Gegenmaßnahmen, schafft Raum für Ausnahmezustände und dient der Rechtfertigung von kostspieligen militärischen und geheimdienstlichen Beschaffungsmaßnahmen. Freilich gehören psychologische Kriegsführung, Spionage, elektronische Kriegsführung und die Zerstörung von Kommunikationsnetzen seit langem zur Kriegsführung. Bereits seit den 1980er Jahren wurde über den Einbruch in gegnerische Computernetze berichtet, hinzugetreten sind in jüngerer Zeit die systematische Nutzung von Computerviren gegen IT-Netze und Generatoren für elektromagnetische Pulse (Jammer).

Der Begriff Cyberwar konnotiert eine diffuse, gleichwohl umfassende Bedrohung auf kritische Infrastrukturen, die Manipulation von Kommunikation, vor allem aber assoziiert er die Furcht vor einem Verlust über das eigene „Bewusstsein", d.h. externe Kontrolle über die Psychologie von Großgruppen. Zu Beginn der 1990er Jahre erdachte der IT-Sicherheitsexperte Winn Schwartau das Szenario eines „‚*electronic Pearl-Harbour*'" (Schwartau in Rid 2016: 307). Zunächst im Pentagon und anschließend in Kreisen der Politik erschütterte das Szenario eines Cyberwar das Vertrauen der USA darauf, ihre nationale Sicherheit überhaupt noch schützen zu können. Die „*first large state-on-state cyber attack*", die russische Spionageoperation „*Moonlight Maze*" gegen US-Forschungseinrichtungen, Ministerien und Regierungsbehörden, die 1998 begann, deklarierte die Clinton-Administration um die Jahrtausendwende zum ersten „Cyberkrieg", einschließlich des befürchteten Szenarios eines elektronischen Pearl-Harbour (Rid 2016: 319). Die exzessive Angstkultur zeichnet in besonderem Maße die USA, Russland und China aus, und sie lebt im Umfeld der Einführung des Mobilfunkstandards 5G zu neuer Höchstform auf: In den USA fürchtet man, China könnte bald die von Edward Snowden enthüllten NSA-Methoden gegen die USA selbst zur Anwendung bringen. Technologisch weniger potente Staaten können bestenfalls den zweifelhaften Ruhm genießen, Objekt der Spionage mehrerer konkurrierender Geheimdienste zu sein.

In der Rede vom Cyberwar verbinden sich atavistische Bilder einer totalitären Welt aus den Romanen „1984" (George Orwell, 1949), „Fahrenheit 451" (Ray Bradbury, 1953), „*The Manchurian Candidate*" (Richard Condon, 1959) mit Vorstellungen einer künstlichen Intelligenz, die die Mensch-Maschine-Grenze auflöst (erstmals im Alan Turing-Test von 1950) und damit die „liberale" Vorstellung menschlicher Autonomie und Selbstbestimmung infrage stellt. Ein solchermaßen imaginierter Feind lässt sich nicht mehr externalisieren, als äußere Bedrohung konzeptualisieren, er ist „unter uns", „in uns", ein Virus mit extremer Mutationsfähigkeit, angewandter Konstruktivismus (die Welt als Narrativ), ein

selbstlernendes Programm oder ein ständig präsenter „Dritter".[3] Cyberwar ist zu einer Chiffre der Bedrohung, für eine fundamentale Verunsicherung über die Möglichkeit rationaler Selbststeuerung geworden und damit des Verlustes von menschlicher Autonomie und Souveränität. Die kollektiven Subjekte von Demokratie – der Demos – und die individuellen Rechtssubjekte (mit Schuldbewusstsein und Schuldfähigkeit) können sich, so die Befürchtung, in einer Welt globalisierter Kommunikation mit ferngesteuerten „Echokammern" nicht mehr selbst konstituieren. Im Unterschied zu den Angstbildern einer totalitären Bewusstseinskontrolle während des „Kalten Krieges" ist die Gewissheit eigener westlicher Überlegenheit – normativ, wissenschaftlich-technologisch und politisch – abhandengekommen, dies potenziert die schaurige Attraktivität der Rede vom Cyberwar.

Doch ist die Rede vom Cyberwar, insbesondere in den USA, nur eine Ausgeburt der selbstinteressierten Bedrohungsindustrie, ein imaginierter Mythos, oder gibt es Indikatoren und Standards für die Bestimmung von Verwundbarkeit und Bedrohungen im Cyberspace? Wie beeinflussen sich Sicherheitsdiskurse und Cyber-Strategien? Und was ist das Ziel einer Eindämmung von Gefährdungen – erhöhter Schutz, Resilienz, die Eskalationsdominanz oder Abschreckung? Wie kann Normenbildung zur Verteidigung digitaler Freiräume beitragen? Welche Werte, Normen und Praktiken sollten die deutsche Innen- und Außenkulturpolitik anleiten?

1.2 Cyberangriffe auf den zoon politikon

Die Welt des Cyberspace eröffnet technische Möglichkeiten der Kommunikation und der Einflussnahme, die auf die Souveränität, die Autonomie, die Selbstbestimmung und Urteilskraft des zoon politicon zielen. Cyberspace besteht aus dem technischen Medium Internet und zugleich dem sozialen Raum, der sich aus der Nutzung der Technologie durch Menschen ergibt. Das Internet ist ein Informations- und Kommunikationsraum, ein Feld für wirtschaftliche Aktivitäten sowie für die strategische Beeinflussung von Öffentlichkeit.

Während das Internet und die sozialen Netzwerke zunächst als Reich der unbegrenzten Informations- und Meinungsfreiheit, der Ermächtigung zur Selbstorganisation, als anti-elitär und als vernetzte Demokratie begrüßt wurden, sind die Möglichkeiten der staatlichen und kommerziellen Ausforschung von Individuen, von Manipulation und Subversion im Zeitverlauf exponentiell gewachsen (Deibert 2015; Rid/Buchanan 2018;

[3] vgl. Ian McEwans Roman „Machines like me", London 2019.

Singer/Brooking 2018). Technologische Möglichkeiten eröffnen ein ungeahntes Potenzial der Überwachung und Manipulation. Autoritäre, aber auch demokratische Regime streben danach, personenbezogene Daten und Informationen systematisch abzuschöpfen, zu kontrollieren und zu steuern – die Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden haben das Ausmaß flächendeckender, mitnichten nur anlassbezogener Überwachung erstmals ins Bewusstsein einer breiteren Öffentlichkeit gerückt und eine Debatte über den Überwachungsstaat ausgelöst. Die staatliche Kontrolle des Internet wurde im Zuge des „Krieges gegen den Terror" erheblich ausgeweitet, sie beschränkt sich jedoch nicht mehr auf dieses Feld.

Daten sind das Öl des 21. Jahrhunderts, wer über sie verfügt, kann die Präferenzen von Konsumenten und Wählern infolge von „*Profiling*" steuern. Insbesondere autoritäre Regime versuchen, eine Art Informationsautokratie zu errichten, Informationsflüsse zu kontrollieren und die Hegemonie systemstützender Werte gegenüber der eigenen Bevölkerung zu erlangen, aber den Cyberraum auch für außenpolitische Einflussnahme aktiv zu nutzen. Als autoritäre Regime das Internet nicht nur als Bedrohung, sondern als Instrument der Machtausübung entdeckten, setzten Debatten um die Abwehr ausländischer Einflussnahme ein.

Doch wie soll eine Grenze zwischen Diskursfreiheit und Meinungsvielfalt auf der einen und Abwehr von illegitimer Einflussnahme auf der anderen Seite gezogen werden? Wenn Demokratien sich vor der Medienpolitik von Autokraten schützen, werden autoritäre Regime dann nicht erst recht jegliche äußere Einflussnahme, z.B. über politische Stiftungen oder Medien, als Informationskrieg bezeichnen und mit Repressionen belegen? Die Grenzen zwischen legitimer Informationspolitik, Beförderung von Werten und illegitimer, manipulativer oder bedrohlicher Einflussnahme sind mitnichten klar gezogen, eine Verständigung über Regeln der Angemessenheit findet international nicht statt. Werden politische Stiftungen oder Massenmedien (z.B. die Auslandsprogramme der Deutschen Welle) in ihrem Wirken beeinträchtigt, kommt es meist zu ad-hoc-Anpassungen oder temporären Kompromissen, eine Verständigung über die Grenze zwischen lässlicher und ungebührlicher Einflussnahme findet jedoch nicht statt; Gleiches gilt für die Einflussnahme mit Hilfe digitaler Medien.

Die „Systemgrenze" zwischen autoritärer und demokratischer Informations- und Datenkontrolle ist diffus, und zwar gerade weil sich auch westliche Sicherheitsapparate, Politiker und kommerzielle Datensammler nicht in einen strukturellen Nachteil gegenüber der Datenkontrolle à la China bringen wollen. Auch Demokratien wollen im „Aus-

nahmezustand“ souverän über kritische Informationsflüsse bestimmen können, und worin dieser „Ausnahmezustand“ gesehen wird, hängt in hohem Maße von der wahrgenommen Bedrohung der normativen, moralischen oder politisch-argumentativen Lufthoheit ab. Die Diskussion um „Resilienz“ handelt somit nicht nur vom Schutz vor verfassungsfeindlicher Mobilisierung, d.h. dem Schutz vor strafbaren Handlungen, sondern der Definition und damit Einschränkung dessen, was als legitime Artikulation auf dem öffentlichen Markt der Meinungen präsentiert werden darf.

2. Cyber-Sicherheitsdiskurse im internationalen Vergleich

Das Verständnis von Sicherheit ist gesellschaftlich konstruiert und der Begriff kulturell aufgeladen. Sicherheit für wen, von wem und wovor? Was als Sicherheitsbedrohung wahrgenommen wird, ist das Ergebnis öffentlicher Diskurse und von Bedrohungs- und Risikowahrnehmungen des Sicherheitsestablishments (von Boemcken 2013). Daran beteiligen sich Vertreter der Sicherheitsorgane, Strafverfolgungsbehörden, Juristen, Medien, Kulturschaffende, Menschenrechtsgruppen, Geheimdienste, Lobbyisten, Sicherheitsfirmen, Computer-Clubs, Hacker, Parteien und Parlamente. Die Diskurse sind durchzogen vom Ruf nach Freiheit, insbesondere der Meinung und des Informationszugangs, von kommerziellen Interessen, politischen Kontrollansprüchen, von Kosmopolitismus auf der einen und Protektionismus auf der anderen Seite. Der Schutz von Grundrechten, die kommerziellen Interessen von Internethändlern, die organisierte Kriminalität und die Kontrollansprüche von Sicherheitsapparaten prallen in diesen Diskursen aufeinander.

Diskurse finden in internationalen und nationalen Kommunikationsräumen und Diskursgemeinschaften statt. Was als Bedrohung für Demokratie und Sicherheit wahrgenommen wird, hat immer auch mit kulturellen Prägungen von Diskursen zu tun. In Staaten wie den USA, Russland, China, der Europäischen Union oder Deutschland werden Diskurse deshalb unterschiedlich geführt. Gesellschaften mit hoher Bewertung von Sicherheit im Verhältnis zu Selbstentfaltungswerten nehmen eher Einschränkungen der informationellen Selbstbestimmung hin als Gesellschaften, die liberale, postmaterialistische Werte hoch schätzen. Was als Bedrohung kollektiver Normen wahrgenommen wird, hängt von diskursiven Konstruktionen und hegemonialen Diskursen ab. Global lässt sich eine „Versicherheitlichung" von öffentlichen Diskursen, eine Militarisierung des Cyberraums beobachten (vgl. Craig/Valeriano 2016). Die „Versicherheitlichung" der Diskurse gilt für die USA, China und Russland, sie greift auch auf Europa über und strahlt auf andere Staaten ab. Wer die Diskurshegemonie dauerhaft behaupten kann ist nicht ausgemacht. Die Kontrollansprüche des Staates nehmen jedenfalls global zu.

USA

In den USA wird von Militärs und Geheimdienstlern ohne Scheu von Cyberwar gesprochen, so als ob man die Logik des Krieges auf die digitale Welt anwenden möchte. Die Cyberwelt wird vielfach als ein Feld der Kriegsführung gegen andere Staaten angesehen und zwischen innerem Feind und äußerem Feind nicht mehr prinzipiell unterschieden. Militärs operieren im Cyberspace zusehends mit Methoden, die denen von Geheimdiensten gleichen. Gemeinsame Operationen (*joint operations*) von Geheimdiensten und Militärs häufen sich. Cyberoperationen in Friedenszeiten beruhen auf Verschleierung, d.h. sie

werden im Stil von Geheimdienstoperationen oder verdeckten Operationen durchgeführt, um die zur Verfügung stehenden Optionen für kompetitives und aggressives Verhalten zu erweitern oder im Kriegsfall militärische Operationen zu unterstützen. Die Verhaltensmuster sind noch kein Krieg, können jedoch mitnichten als friedlich bezeichnet werden (Gartzke/Lindsay 2015: 346; vgl. Kello 2018: 56). Dass Russland im Bereich der Cyber-Spionage und der Einflussnahme umtriebig ist, ruft hierzulande gern mediale Empörung hervor (Popescu 2018), freilich gehören die USA, China (vgl. Lindsay et al. 2015), Frankreich, Großbritannien, Iran (vgl. Anderson/Sadjapour 2018) und Nordkorea (vgl. Kello 2018: 146-157) ebenfalls zu den aktivsten staatlichen Cyberakteuren.

Die Führung von sogenannten Informationskriegen reicht von der Beeinflussung von Medien vor einem bewaffneten Konflikt über das Ausspähen von Daten (Spionage) bis zum Einsatz von Schadsoftware und der Zerstörung von Infrastrukturen oder der Ausschaltung von elektronischen Geräten durch Erzeugung eines elektromagnetischen Impulses. Neue technische Mittel erweitern die Kampfzone, um „Informationskriege" zu führen. Ruhmann schreibt: „Dank der im Internet inhärent vorhandenen Manipulationsmöglichkeiten mit erheblichem Schadenspotential ist die Vielfalt potenzieller Gegner bei einer Cyber-Kriegsführung kaum mehr begrenzt."(Ruhmann 2012: 28-31, auch zum folgenden) 1996 veröffentlichte die US Army mit dem Field Manual 100-6 erstmals eine Doktrin für „*Information Operations*", die dann 2003 durch das Field Manual 3-13 ersetzt wurde. Demzufolge sind Informationsoperationen

> „… die Anwendung von Kernfähigkeiten der elektronischen Kriegsführung, Computernetzwerkoperationen, psychologischen Operationen, militärischen Täuschungsmanövern und Operationssicherheit, kombiniert mit bestimmten Unterstützungs- und ähnlichen Fähigkeiten, um Informationen und Informationssysteme zu beeinträchtigen oder zu verteidigen und Entscheidungsprozesse zu beeinflussen".[4]

Die Militarisierung des Cyberraumes (und des Diskurses darüber) eröffnet somit ein weites Repertoire des Interventionismus (vgl. generell dazu Hansel 2013).

Mitte Juni 2019 berichtete die New York Times, dass amerikanische Geheimdienste Malware, also Schadsoftware, in das russische Stromnetz eingeschleust hätten. Es wäre eine Warnung an Präsident Putin gewesen, wonach man im Falle eines größeren Konflikts zu einem Cyberangriff fähig und bereit sei (Sanger/Perlorth 2019). Die Sabotage kritischer

[4] Department of the Army, Headquarters (2003): Field Manual 3-13 (FM 100-6) Information Operations: Doctrine, Tactics, Techniques, and Procedures. November, S. 1-13.

Infrastruktur – oder die Drohung damit – eröffnet eine mögliche Aktions-Reaktions-Spirale ungehemmter Angriffsfähigkeit und unterminiert jene Vertrauensbestände, die nach dem Ende des Ost-West-Konfliktes zeitweilig möglich schienen.

China

Das politische Regime Chinas sieht in der Kontrolle des Internets bzw. der sozialen Medien vor allen Dingen ein Mittel, um sich gegen „unregulierte Freiheit" bis hin zu Protesten präventiv zu wappnen – ein Medium der Sozialkontrolle. In einem Aufsatz zur chinesischen Cyberpolitik optiert der chinesische Generalmajor Hao Yeli für „Cyber-Souveränität". Die technische Infrastruktur des Internet solle Interkonnektivität ermöglichen (Multilateralismus sei auf dieser Ebene möglich), auf der Ebene der Internet-Plattformen müsse man hingegen ein „dynamisches Gleichgewicht" zwischen Freiheit und Ordnung finden, wenn es aber um das politische Regime, Gesetze, die politische Sicherheit und die Ideologie ginge, würde China seine Souveränität auch im Cyberraum schützen (Yeli 2017: 113ff.). China schreibt sich den Begriff *Information Warfare* zugute und hat ähnlich weitreichende Konzepte wie das US-Militär entwickelt, es setzt auf einen „Volksinformationskrieg". Das Regime strebt nach „Cyber-Souveränität" – ein Rollenmodell, das von anderen Autokratien imitiert wird.

Russland

Die erste russische Cyber-Sicherheitsdoktrin von 2000 nahm noch keinen Bezug auf die Informationsvernetzung und das Internet, doch die zweite Cyber-Sicherheitsdoktrin von 2016 sprach explizit vom Schutz der nationalen Interessen der Russischen Föderation im Cyberspace, sie verknüpfte diese mit der russischen Sicherheitsstrategie und der Verteidigungspolitik und stellte vor allem die politischen und militärischen Sicherheitsinteressen in den Mittelpunkt. Russland müsse sich gegen Hackerangriffe und Medienkampagnen aus dem Ausland zur Wehr setzen, es solle sich dagegen erwehren, dass Staaten versuchten, zu militärischen Zwecken Einfluss auf die russische Informationsinfrastruktur zu nehmen.[5] Russland setzt vor allem auf die psychologische und elektronische Kriegsführung, verfügt aber auch über Kapazitäten für moderne Cyber-Kriegsführung.

Deutschland

In Deutschland werden vor allem Diskussionen um die Datensicherheit und um informationelle Selbstbestimmung geführt, ferner, ob und wie die defensiven Fähigkeiten ausge-

[5] https://www.heise.de/newsticker/meldung/Russland-mit-neuer-Doktrin-gegen-Hackerangriffe-3562470.html.

baut werden sollten, weil erhebliche Schwachstellen insbesondere infolge der Enthüllungen von Edward Snowden im Jahre 2013 sichtbar geworden sind. Die Angriffe auf die Netzwerke des Bundestags und des Auswärtigen Amts verdeutlichten die Sicherheitslücken (vgl. Beuth et al. 2017; Mascolo et al. 2018). Einerseits wurde sichtbar, dass Cybersicherheit mehr Anstrengungen erfordert, andererseits herrschen Vorbehalte, ob der Cyberraum für offensive Operationen genutzt werden darf. Darüber hinaus gibt es in Deutschland einen Richtungsstreit, was der Cybersicherheit am dienlichsten sei. Vor dem Hintergrund des Aufbaus militärischer Cyberfähigkeiten und der neugegründeten „Zentralen Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS) sowie der geplanten Schaffung einer „Agentur für Innovation in der Cybersicherheit", die beide auch offensive Cybertechnologien erforschen und fördern sollen, sehen Matthias Schulze (Stiftung Wissenschaft und Politik) und Sven Herpig (Stiftung Neue Verantwortung) einen Paradigmenwechsel in der deutschen Haltung zur Cybersicherheit. Ihnen zufolge würden offensive Cyberoperationen bzw. entsprechende Cyberfähigkeiten gegenüber der Stärkung der allgemeinen IT-Sicherheit priorisiert (Schulze/Herpig 2018).

Der Koordinierungsstab im Auswärtigen Amt für Cyber-Außenpolitik setzt sich für das Internet und Digitalisierung als Räume der Freiheit, von Chancen und für Sicherheit ein. Ziel dieser Politik ist es, so heißt es vom Auswärtigen Amt,

> „die Sicherheit des Cyber-Raums zu gewährleisten und aus der zunehmenden Digitalisierung entstehende Bedrohungen einzudämmen; universelle Menschenrechte wie den Schutz der Privatsphäre, der Meinungs- und Pressefreiheit auch im Internet zu gewährleisten und Freiheitsräume auszubauen und das Spannungsverhältnis zwischen diesen beiden Zielen auszugestalten."[6]

Weiter formuliert das Auswärtige Amt:

> „Cyber-Außenpolitik soll deutsche Interessen und Vorstellungen in Bezug auf Cyber-Sicherheit in internationalen Organisationen koordinieren und verfolgen, zum Beispiel in den VN, der OSZE, dem Europarat, der OECD und der NATO. Wir engagieren uns für die Stärkung eines gemeinsamen europäischen Handlungsrahmens bei Cyberbedrohungen und setzen uns für ein koordiniertes Vorgehen im Kreis gleichgesinnter Staaten gegen konkrete Bedrohungen und aggressive Cyberkampagnen ein."

[6] https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik.

Schutz von Menschenrechten, Erhalt und Erweiterung von Freiheitsräumen, internationales Recht, verantwortungsvolles Staatenhandeln, vertrauensbildende Maßnahmen und das Eintreten für deutsche sowie europäische Ansätze bei der Standardsetzung und Ausgestaltung der Weltordnung des „digitalen" Zeitalters lauten die entscheidenden Stichworte.

***

Insbesondere autoritäre bzw. semi-autoritäre Regime wie Russland, China, Saudi-Arabien oder die Türkei beeinflussen über Nachrichtensender, durch kulturelle Außenpolitik, soziale Netzwerke, Einflussagenten, Diasporagemeinden und Austauschprogramme die öffentliche Meinung in westlichen und nicht-westlichen Staaten (Deibert 2015; Cardenal et al. 2017). Sie mischen sich in Wahlkämpfe ein und versuchen, politische Kontroversen in der Öffentlichkeit westlicher Staaten auszunutzen, oder sie verbreiten gezielt Desinformation. Eine Vielzahl autoritärer Staaten nutzen technische Mittel und illegale Maßnahmen, um Informationen im Internet zu kontrollieren und um Oppositionsgruppen, Regimekritiker und zivilgesellschaftliche Gruppen zu überwachen, auszuspionieren und zu verfolgen (Rid/Buchanan 2018: 9).

Bei „niedrigschwelligen" Aktivitäten der Überwachung kommen häufig irreguläre bzw. nicht-staatliche Akteure ins Spiel. Die Vereinigten Arabischen Emirate haben so z.B. Ex-NSA-Mitarbeiter eingestellt, um Journalisten und Regimekritiker auszuspionieren und ihre eigenen Fähigkeiten auf dem Feld auszubauen (Bing/Schectman 2019). Autoritäre Regime schotten sich gegen interne Kritiker ab, indem sie Massenmedien und Journalisten unter Kontrolle bringen. Im Innern fürchten autoritäre Führungen wie die Kommunistische Partei Chinas die sozialen Folgen der wirtschaftlichen Liberalisierung. Ein Legitimitätsverlust und Instabilität könnten die Folge sein. Die Verbreitung des Internet erhöht die Verwundbarkeit von autoritären Regimen, zugleich bieten sich neue Möglichkeiten der Sozialkontrolle. Über die „*World Internet Conference*" versucht China z.B. seit Jahren, seine Konzepte für eine „sichere" und digitale Welt zu propagieren und zu vermarkten. Es findet Interessenten vor allem in autoritären Entwicklungsländern. Die Dynamik des chinesischen Autoritarismus ist nicht zuletzt im geschickten Umgang mit dem Internet begründet (Lu 2018).

China, Russland, Kasachstan, Kirgistan, Tadschikistan und Usbekistan brachten 2015 einen Resolutionsentwurf zur Anwendbarkeit von Recht auf den Cyberspace und Regeln in die UN Generalversammlung ein, der Teile des „*Shanghai Cooperation Organization's International Code of Conduct on Information Security*" enthielt. Besagter Verhaltenskodex ist

dazu angetan, „online"-Menschenrechte zu konterkarieren und Meinungsfreiheit einzuschränken (Grigsby 2018; Deibert 2015: 70f.). Das Narrativ des Codes betont die staatliche Souveränität und Territorialität in der digitalen Welt und ist beherrscht von den Imperativen der Geheimdienste, nationaler Sicherheit und der Regimestabilität, wie Sarah McKune schreibt (McKune 2015). Staaten wie China investieren erheblich in Bemühungen, eine neue digitale chinesische Mauer, eine Firewall zu errichten, um nationale Kontrolle über den Informations- und Kommunikationsraum des Internet zu erlangen. In dieser Hinsicht befinden wir uns in einem neuen Systemkonflikt: Es geht um die politische Kontrolle der öffentlichen Meinungsbildung. Wie man an diesen Entwicklungen und Debatten sieht, ist der Cyberraum zum Feld der Auseinandersetzung um Gesellschaftsordnungen geworden. Die Auseinandersetzung zwischen offenen, liberalen Gesellschaften und Kontrollregimen findet im Cyberraum statt.

Sind zwischenstaatliche und zwischengesellschaftliche Interaktionen von Aggression, Wettbewerb und Konflikt geprägt oder lässt sich die Interaktion im Cyberraum normativ und regulativ einhegen? Es geht letztlich um die Verteidigung informationeller Selbstbestimmung und einer offenen, pluralen Gesellschaft, einer Gesellschaft, in der es einen freien und fairen Austausch von Meinungen gibt, um Zugang zu unterschiedlichen Meinungen und um verlässliche, überprüfbare Informationen. Dem stehen jene Kräfte gegenüber, die den öffentlichen Raum Internet, insbesondere die personenbezogenen Daten, kontrollieren, manipulieren und ausbeuten wollen, also eine Art „Orwell 1984" anstreben. Die Auswärtige Kultur- und Bildungspolitik kann einen Beitrag dazu leisten, dass die demokratische, selbstbestimmte Gesellschaft und das Recht auf informationelle Selbstbestimmung gegen Manipulation und Kontrolle verteidigt werden.

3. Subversion im Cyberraum: Manipulieren, Misstrauen sähen, desorientieren

Subversion zielt auf die Unterminierung von politischer Autorität oder staatlicher Integrität, sie will Zweifel an der Glaubwürdigkeit von Institutionen, Organisationen und Informationen nähren; Subversion strebt nach Zersetzung des Legitimitätsglaubens, nach Erosion des sozialer Zusammenhaltes, dazu gehört neben der Unterminierung von Geheimdiensten bzw. deren Delegitimierung als „Beschützer" demokratischer Ordnungen auch das Säen von Misstrauen in die zugrundeliegende technische Infrastruktur (Rid/Buchanan 2018: 8 ff.). Zur Subversion gehören all jene Bestrebungen oder Darstellungen, die das Vertrauen in demokratische bzw. rechtsstaatliche Prozesse und Institutionen gezielt in Frage stellen, und zwar mit dem Ziel, die Ordnung selbst zu untergraben. Brattberg und Maurer differenzieren zwischen Angriffen auf Parteien, auf Accounts von Politikern und auf die Wahlinfrastruktur, zwischen Kampagnen und der Nutzung sozialer Medien bzw. konventioneller Medienorganisationen (Brattberg/Maurer 2018: 4). Sie unterscheiden zwischen Versuchen, die Präferenzen von Wählerinnen und Wählern zu verändern, Wahlen zu manipulieren und die Wahlbeteiligung zu beeinflussen (Brattberg/Maurer 2018: 27 f.).

Politische Subversion meint die Unterwanderung einer bestehenden Ordnung, sie kann sich prinzipiell sowohl gegen demokratische wie autoritäre Regime richten. Subversion kann der Auftakt für eine Revolution sein oder sich zu einer gewaltfreien oder gewaltsamen Kampagne fortentwickeln (Rid 2017: 121.). Sie operiert mit verdeckten Methoden, nicht unter Bedingungen eines fairen Wettbewerbs der Ideen, d.h. Subversion setzt sich nicht den Rechtfertigungszwängen einer demokratischen Gesellschaft aus, sondern operiert mit Falschmeldungen, Gerüchten, der Unterdrückung von Nachrichten, der Illusion von fiktiven Mehrheiten bzw. sozialen Massen (z.B. durch Troll-Fabriken oder automatisierte „Bots" in sozialen Medien, durch organisierte „*shit storms*" u.ä.) (Chen 2015). Subversion entzieht sich dem offenen, dem fairen Wettbewerb, sie operiert gleichsam „unterhalb der Gürtellinie". Angriffsziel der Subversion sind Verstand und Herzen von Menschen. Die Mobilisierung von Emotionen, die gezielte Ansprache des „schnellen Denkens" – schnell, automatisch, emotional, stereotypisierend, unbewusst, stets aktiv – durch soziale Medien ist ein wesentlicher Modus operandi von Subversion. Der Psychologe Daniel Kahneman hat die Vielfalt kognitiver Mechanismen als Parallelität von „schnellem" und „langsamem Denken" beschrieben – Mechanismen, die sich Manipulatoren der sozialen Medien gezielt zu Eigen machen. Es werden kausale Zusammenhänge zwischen unvollständigen, aber zufällig verfügbaren Informationen hergestellt. Zudem wird das eigene „Wissen" gegenüber anderslautenden Fakten überbewertet, während

eigene Erwartungen massiv die Rahmung (das „Framing“) von Entscheidungen beeinflussen (Kahneman 2012).

Die kognitiven Mechanismen des „schnellen Denkens“ bieten einen Ansatzpunkt für Subversion. Subversion macht sich die Ästhetik und die Emotionalität von Subkulturen zu eigen, sie tritt im Gestus des Protestes, der Gegenkultur, als Sprachrohr unterdrückter Meinungen, „gegen das Establishment“, im Namen „des Volkes“ auf, sie greift moralische Ordnungen an, zieht Genugtuung aus Destabilisierung, delektiert sich an Krisen, die als Beleg der eigenen moralischen Überlegenheit und Urteilskraft fungieren, und ruft nostalgisch nach Rückkehr zu einer verlorenen „Normalität“ in der Vergangenheit. Die normativen Kräfte des Gegners sollen durch Demoralisierung und Destabilisierung gegen diesen selbst gerichtet werden, d.h. ihn desavouieren. Subversion kommt ohne Programm oder Agenda aus – eine Inquisition im Namen der imaginierten Massen, des Volkes, einer Meute, die bedient werden möchte. Wer mit dem Gestus der Subversion auftritt, kennt stets „die Wahrheit“, er deckt sie auf, zieht „der Lügenpresse“ die Maske vom Gesicht. Subversion operiert mit dem Standardrepertoire dessen, was seit einigen Jahren pathologisierend und derogativ als Populismus bezeichnet wird.

Cyberoperationen können der Erlangung sensibler Daten und Informationen dienen, mit denen das Vertrauen der Bevölkerung in einen Politiker, eine Partei oder eine politische Institution untergraben wird, wie beispielsweise bei den US-Präsidentschaftswahlen 2016. Diese Form der Cybersubversion kann – wie auch beim Brexit-Referendum im Juni 2016 – auf Falsch- und Desinformation von Nutzerinnen und Nutzern sozialer Medien und traditioneller Medienkanäle aufbauen, die dann über soziale Medien und die Nutzung von Bots weiterverbreitet werden. Cybersubversion kann sich auch gegen die technische Infrastruktur von politischen Institutionen richten, indem sie deren korrektes Funktionieren oder die Integrität von Daten beeinflusst. Über den technischen Umweg wird so das Vertrauen der Bevölkerung in das korrekte Funktionieren politischer Institutionen beeinträchtigt. Die folgenden Beispiele zeigen, wie Spionage und Sabotage im Cyberraum zur Subversion genutzt werden.

US-Präsidentschaftswahlen 2016

Subversion wurde im Jahre 2016 durch die gezielte Wahlbeeinflussung der US-Präsidentschaftswahlen durch Russland von einem Schreckgespenst zur Realität. Russische Agenten der Einheit 26165 des Militärgeheimdienstes GRU drangen im Frühjahr 2016 in die Netzwerke und E-Mail-Konten von Mitarbeitern der Präsidentschaftskandidatin Hillary Clinton ein, spionierten diese aus und stahlen E-Mails und Dokumente. Bereits

2008 hatten China und Russland im Vorfeld der US-Präsidentschaftswahlen Republikaner und Demokraten ausspioniert. Ab Mitte Juni 2016 veröffentlichten Agenten des russischen Militärgeheimdienstes GRU (Einheit 74455) unter der fiktiven Online-Identität „Guccifer2.0", deren Wordpress Blog, auf der Webseite „DCLeaks.com" und später durch Weitergabe an die Enthüllungsplattform „Wikileaks" Dokumente und E-Mails der Demokraten (*United States District Court for the District of Columbia* (CftDoC) 2018a: 13-19). Neu am russischen Vorgehen war die gezielte Veröffentlichung von illegal erworbenen Informationen.

Mehr als ein Jahr vor der Anklage von 12 russischen GRU-Agenten durch die US-Justiz im März 2018 urteilten die amerikanischen Sicherheitsbehörden und Nachrichtendienste, dass die russische Regierung eine Einflusskampagne mit dem Ziel der „Untergrabung des öffentlichen Glaubens" an den demokratischen Prozess und die Diskreditierung der Präsidentschaftskandidatin Hillary Clinton angeordnet habe (*Office of the Directorate National Intelligence* (ODNI) 2017: ii.). Ein US-Gericht klagte die als „Trollfabrik" bekannte und in Sankt-Petersburg ansässige „*Internet Research Agency*", zwei weitere Firmen und dreizehn für diese Organisationen tätige russische Staatsbürger wegen Verschwörung an. Die Angeklagten nutzten ab 2016 Accounts unter falscher Identität zur gezielten Verbreitung von herabwürdigenden Informationen über Clinton, verbreiteten Falschinformationen, warben für die Wahl Donald Trumps und riefen zu Pro-Trump-Demonstrationen auf (CftDoC 2018b: 21 ff.). Die russischen Auslandssender „*Russia Today*" (RT) und Sputnik PR-betrieben ebenfalls eine Kampagne zugunsten von Donald Trump (ODNI 2017: 3f.; 6- 12).

Brexit

In Großbritannien unterstützten die russischen Sender RT und Sputnik im Jahr 2016 Inhalte gegen einen Verbleib in der EU. Mit seinen Accounts hätten RT und Sputnik auf Twitter drei Mal so viel Reichweite gehabt wie die beiden offiziellen „*Leave*"-Kampagnen zusammen, sie hätten überwiegend Artikel mit deutlich übertriebenen und verzerrenden Inhalten zur EU und dem Referendum verbreitet (Harris/Feldberg 2018). Einer Studie der City University of London zufolge sollen ca. 13.500 „Bots" auf Twitter für einen Ausstieg Großbritanniens aus der EU geworben und dazu beigetragen haben, Identitäten zu polarisieren (Bastos/Mercea 2017: 2). Die „Bots" waren möglicherweise nicht wahlentscheidend, aber sie fungierten als „Echo-Kammern" für Menschen mit geteilten Voreinstellungen (Gorodnichenko et al 2018: 23). Gorodnichenko et al. schlussfolgern, dass die Verstärkung ideologischer Polarisierung in sozialen Medien einen gesellschaftlichen Konsens über wichtige Themen erschwert (Gorodnichenko et al 2018: 23).

Insgesamt scheinen Bots umso erfolgreicher zu wirken, je mehr sie bestehende Vorurteile bedienen. Zwei Studien verweisen darauf, dass russische Desinformationskampagnen in europäischen Ländern einen systematischen Charakter haben und sich auf eine Vielfalt an Medien erstrecken (Meister 2018; Spahn 2018). Umgekehrt wurde die britische „*Integrity Initiative*", die auf russische Desinformationskampagnen aufmerksam machen wollte, von der pro-russischen Hackergruppe „Anonymous" gehackt und das dann geleakte Material von russischen Staatsmedien, darunter Sputnik und RT Deutsch, und pro-russischen Medien wie Telopolis sowie den sogenannten „Nachdenkseiten" in weitgehend wortgleichen Wortbeiträgen als anti-russische Propaganda denunziert.[7] Das Muster: Wer Desinformation aufdeckt, kann demnach selbst nur ein Einflussagent sein. Andere autoritäre Regime imitieren das russische Vorgehen. Die private IT-Sicherheitsfirma „Fireeye" deckte im August 2018 ein seit 2017 aktives Netzwerk von intransparenten Nachrichtenseiten auf. Ein vom Iran unterstütztes Netzwerk, das sich an ein Publikum in den USA, Großbritannien, Südamerika und den Nahen Osten richtet, verbreitet sowohl anti-saudische, anti-israelische als auch pro-palästinensische Meinungen (Fireyee 2018).

Ukrainekonflikt

Die Anklage von US-Sonderermittler Robert Mueller vom 28. September 2018 gegen die Bürgerin von Sankt Petersburg, Elena Alekseevna Chusjainova, dokumentierte, dass die russischen Bemühungen, Einfluss auf politische Prozesse und Wahlen in den USA, in EU-Staaten und in der Ukraine zu nehmen, auch nach den Enthüllungen zur Wahlmanipulation im Jahre 2016 weitergingen (*United States District Court for the Eastern District of Virginia* (US-DCftEDoV) 2018). Chusjainova soll Chefbuchhalterin des seit 2014 aktiven „*Project Lachta*" gewesen sein, zu dem u.a. die im Februar 2018 angeklagte „*Internet Research Agency*", weitere Tarnfirmen und Hunderte von Angestellten gehörten (US-DCftEDoV 2018: 3f). Der Oligarch und Putin-Verbündete, Evgeniy Viktorovič Prigožin, fungierte als Finanzier der Operation. „Project Lachta", dessen Budget zwischen Januar 2016 und Juni 2018 bei über 35 Millionen US-Dollar lag, sollte die US-Öffentlichkeit desorientieren und polarisieren (US-DCftEDoV 2018: 12f.). Die Beispiele illustrieren das Portfolio und Methoden der Einflussnahme mittels sozialer Medien oder Internet-Plattformen auf politische Prozesse in westlichen Demokratien.

[7] https://www.extremnews.com/berichte/weltgeschehen/a8fd170ced64d8b; https://www.nachdenkseiten.de/wp-print.php?p=48281.

Im Internet werden soziale oder politische Themen bzw. Anlässe von pro-russischen Portalen mit „systemkritischer" Attitüde auch über eine längere Zeit „warm" gehalten – die moralisch rigorosen, stets Allwissenden, im Habitus des Aufklärers auftretenden „Enthüllungsjournalisten", Vollzeit-Blogger bzw. „Experten" folgen durchweg einer Masche: Mit Russland, Syrien oder dem Iran werden Unschuldige angeklagt, während „der Westen" Verursacher allen Weltübels ist. Die recherchefreie Meinungsmache ist kostengünstig, technisch leicht durchführbar, bietet Ego-Shootern eine Bühne auch ohne professionelle Meriten – und hält die Gemeinde der Follower mit täglichen Predigten bei der Fahnenstange.

Im Mai 2014 drang die Gruppe „Cyberberkut", die im Ukraine-Konflikt aktiv ist und Russland zugerechnet wird, in die Computer der ukrainischen Wahlkommission ein (vgl. Hulcoop et al. 2017; National Cyber Security Center 2018; Gorchinskaya et al. 2014). Cyberberkut manipulierte die Software, mit der die Wahlergebnisse aus den einzelnen Bezirken live im Fernsehen übertragen werden sollten derart, dass durch die Veränderung der Übertragung eines Wahlergebnisses in der Gesamtprojektion nicht der pro-westliche Kandidat Petro Poroschenko, der spätere Wahlsieger, sondern eine nationalistische Partei die Wahlen gewonnen hätte (Clayton 2014; Koval 2015: 67). Ohne die eigentlichen Wahlergebnisse zu manipulieren, wäre durch die Manipulation der im Fernsehen übertragenen Wahlergebnisse das Vertrauen der Wähler in die Arbeit der Wahlkommission untergraben worden. Die Sabotage von Teilen der Wahlinfrastruktur (Wahlregister, digitale Wahlberechtigungsregister, Wahlmaschinen und Wahlauswertungssysteme) unterminiert das Vertrauen der Wähler in das Wahlsystem bzw. das Wahlergebnis. Informationen, die zuvor in einer Cyberoperation gestohlen wurden, können öffentlichkeitswirksam im Internet und in sozialen Medien lanciert und mit Hilfe falscher Accounts in sozialen Medien, Bots und über klassische Medien weiterverbreitet werden. Rid und Buchanan bezeichnen dies als „*hack-leak-amplify activities*" bzw. als eine „*hacking-aided influence campaign*" (Rid/Buchanan 2018: 8).

4. Resilienz stärken und nutzen

4.1 Wehrhafte Demokratie

Wie wehrhaft sind Demokratien bei der Verteidigung von öffentlichen Kommunikationsräumen gegen Manipulation durch äußere Einflussagenten, durch Hassreden oder „Volksverhetzung", d.h. gegenüber kommunikativem Verhalten, das geeignet ist, den öffentlichen Frieden zu stören, zum Hass gegen Teile der Bevölkerung aufstachelt, zu Gewalt- oder Willkürmaßnahmen gegen sie auffordert oder die Menschenwürde angreift? Angesichts des Aufstiegs faschistischer Bewegungen in Europa ab den 1920er Jahren kamen erste Überlegungen auf, wie sich demokratische Systeme vor inneren Bedrohungen schützen könnten. Der Staats- und Verfassungsrechtler Karl Löwenstein (1891-1973) prägte den Begriff der militanten Demokratie, der Soziologe Karl Mannheim (1893-1947) sprach von „wehrhafter Demokratie" (Löwenstein 1937a: 423; Mannheim [1943] 1997: 7). Löwenstein optierte für eine starke Regierung, die durch legislative Maßnahmen und Vorkehrungen für den Notstandsfall demokratische Grundfreiheiten und die Verfassung schützt (Löwenstein 1937a: 432). Mit Symbolpolitik und Propaganda habe der Faschismus Teile der Gesellschaft gegeneinander ausgespielt. Löwenstein zufolge nutzte der Faschismus die Demokratie für deren Zerstörung aus. Die Politik müsse deshalb Gesetze erlassen, die sich unmittelbar gegen „faschistische Techniken" richten (Löwenstein 1937a: 429). Er plädierte für einen „Notfallmodus", damit die Regierung im Falle der Blockade oder Sabotage der gewöhnlichen Gesetzgebung das demokratische System schützen kann. Karl Mannheim griff die Idee der wehrhaften Demokratie auf, seine Antwort auf den Aufstieg totalitärer Systeme war die „Planung für Freiheit" (Mannheim [1943] 1997: 5). Neben dem politischen System müsse Planung auch die Wirtschaft umfassen, um soziale Ungleichheiten zugunsten sozialer Gerechtigkeit zu regulieren. Die Demokratie müsse für ihr Überleben wehrhaft sein, schlussfolgerte Mannheim (Mannheim [1943] 1997: 6f.). Unter demokratischer Planung verstand er nicht den Oktroi eines Wertesystems und einer autokratischen „Zwangsjacke sozialer Ordnung", sondern Wehrhaftigkeit (Mannheim [1943] 1997: 7). Doch darf sich Demokratie mit Mitteln wehren, die das demokratische Versprechen, das Urvertrauen in den Demos, zu untergraben drohen, weil „das Volk" populistisch sein könnte?

Das Grundgesetz erklärt: „Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist" (Grundgesetz Art. 20 (4)). „Jeder" kann ein Politiker, ein Amtsträger, ein nichtstaatlicher Akteur sein. Das politische System der Bundesrepublik Deutschland wird vom Bundesverfassungsgericht als streitbare bzw. wehrhafte Demokratie bezeichnet. Eine Verwirkung bestimmter Grundrechte (Art. 18 GG) kann sogar durch das Bundesverfas-

sungsgericht ausgesprochen werden, wenn diese Grundrechte im Kampf gegen die freiheitliche demokratische Grundordnung missbraucht werden. Insbesondere betrifft dies die Presse-, Versammlungs-, die Vereinigungs- und die Lehrfreiheit, das Brief-, Post- und Fernmeldegeheimnis, das Recht auf Eigentum und das Asylrecht. Das Konzept der „wehrhaften Demokratie" schließt extremistische Inhalte und den Nationalsozialismus verherrlichende Symbolik vom politischen Wettbewerb aus. Wehrhafte Demokratie kann zum Verbot verfassungsfeindlicher Parteien und Organisationen führen und im Falle der Notstandsgesetzgebung zu einer erheblichen Einschränkung von Grundrechten.

Das Konzept der streitbaren Demokratie wurde als Antwort auf politischen Extremismus entwickelt, es reicht vom Strafrecht über nicht-strafrechtliche Instrumente wie ein Partei- und Vereinsverbot, Eingriffe in die Versammlungsfreiheit, Zugangsbeschränkungen im öffentlichen Dienst bis hin zu einer demokratietheoretisch hoch problematischen Grundrechtsverwirkung. Deutschland und die USA unterscheiden sich fundamental im Umgang mit nicht-gewalttätigem Extremismus – die USA halten das demokratische Versprechen hoch, während in Deutschland früh zu repressiven Mitteln gegriffen werden kann (Flümann 2015: 406f.). Das Konzept der wehrhaften bzw. der streitbaren Demokratie ist in jedem Fall in hohem Maße begründungspflichtig, um nicht der Legitimation von Kontrolle und Disziplin gegenüber Pluralismus und ergebnisoffenem politischen Wettbewerb zu dienen.

Subversion im Cyberraum kann, vergleichbar Hassreden, zu Straftaten, inklusive Gewalt, aufrufen oder diese verherrlichen. Bei begründetem Verdacht können und sollten der Verfassungsschutz oder der Bundesnachrichtendienst Cybersubversion durch fremde Staaten beobachten und dokumentieren. Es müsste jedoch eine programmatisch-absichtsvolle, greifbare und konkrete Gefährdung der demokratischen Grundordnung, der rechtlichen Grundlagen und des friedlichen Zusammenlebens vorliegen, um repressive Maßnahmen zu rechtfertigen. Ein pauschales Verbot des Zugangs zu Online-Diensten, weil sie aus dem gegnerischen Ausland kommen, ist rechtsstaatlich und demokratisch kaum begründbar. Im Jahre 2017 sperrte die Regierung der Ukraine den Zugang zu mehreren russischen Internetdiensten, darunter beliebte soziale Netzwerke wie VKontakte, das Netzwerk Odnoklassniki und das E-Mail-Portal Mail.ru sowie die russische Suchmaschine Yandex, und machte sich damit selbst zum Advokaten einer geschlossenen Gesellschaft.[8]

[8] https://www.zeit.de/politik/ausland/2017-05/petro-poroschenko-ukraine-russische-webseiten-sperrung; vgl. auch die Beiträge in den Ukraine-Analysen Nr. 186 vom 14.6.2017, www.laender-analysen.de.

4.2 Gesellschaftliche Resilienz

In der Diskussion über den Schutz demokratischer Systeme wird in programmatischen Dokumenten, etwa der Globalstrategie für die Außen- und Sicherheitspolitik der Europäischen Union und dem deutschen Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundesrepublik, der Begriff der Resilienz benutzt, die es zu stärken bzw. aufzubauen gelte (Europäische Kommission 2016; Bundesministerium der Verteidigung (BMVg) 2016). In Bezug auf Cybersicherheit erklärt die Globalstrategie vergleichsweise bescheiden, dass die Europäische Union die technologischen Fähigkeiten stärken möchte, um Bedrohungen gegen die kritische Infrastruktur, Netzwerke und Dienstleistungen „abzuschwächen" (*to mitigate*). Im selben Dokument spricht die Europäische Kommission vage davon, dass sie die Resilienz der Demokratien stärken möchte (Europäische Kommission 2016: 8). Das deutsche Weißbuch sieht in staatlicher und gesamtgesellschaftlicher Resilienz wiederum die Grundlage für eine umfassende Verteidigungsfähigkeit gegen hybride Aktivitäten wie „Cyberangriffe und Informationsoperationen (zum Beispiel Propaganda) [...] sowie Versuche zur politischen Destabilisierung", für die „offene pluralistische und demokratische Gesellschaften" sehr anfällig seien (BMVg 2016: 39). Was Resilienz bedeutet und wie sie hergestellt werden soll, erläutert das Weißbuch indes nicht.

Resilienz ist ein Schlagwort – es meint im weitesten Sinne die Immunisierung gegen systemische Verwundbarkeit. Man könnte Resilienz als Durchhaltevermögen, Krisenbeständigkeit, Stabilität oder als Reproduktionsfähigkeit eines Systems fassen. In welchem Verhältnis Wandlungs- und Anpassungsfähigkeit bzw. Dynamik zur Stabilisierung des Status Quo stehen, lässt der Begriff der Resilienz allerdings offen. Essenziell für Resilienz scheint die Fähigkeit, auf äußere Störungen konstruktiv zu reagieren bzw. diese zu absorbieren, bevor systemische Veränderungen eintreten (Carpenter et al. 2001: 766; Adger 2006: 268; Hagmann 2012: 9). Resilienz wäre dann die Krisen- und Lernfähigkeit eines Systems. Sowohl demokratische als auch autoritäre, hoch entwickelte als auch wenig entwickelte Gesellschaften können sich als resilient erweisen.

Malkki und Sinkonen sprechen von der Fähigkeit zur Absorption, zum Widerstand und zur Reorganisation politischer Prozesse und Wahlen bzw. des breiteren „politischen Lebens" gegenüber subversiver Aktivität von externen Akteuren (Malkki/Sinkonen 2016: 287). Aber was soll eine solcherart verstandene Resilienz bedeuten – die Abschottung gegen Informationen und Meinungen externer Akteure? Würde sich demokratische Resilienz qualitativ von einer „chinesischen Firewall" unterscheiden? Ist es nicht gerade das Kennzeichen offener Gesellschaften, dass sie auf den demokratischen Wettbewerb von Ideen vertrauen statt ihn vorab zu reglementieren? Was bedeutet Resilienz gegen äußere

Einflussnahme, wenn diese Resonanz im Innern findet? Sollen Informationen, Meinungen oder Willensbekundungen deshalb restriktiv behandelt werden, weil sie „von außen" kommen? Wer sollte darüber entscheiden dürfen, dass Einflüsse „von außen" illegitim sind, ohne sich dem Vorwurf der Zensur auszusetzen? Würden autoritäre Regime sich nicht ebenso legitim gegen äußere Einflussnahme wappnen, indem sie das Wirken politischer Stiftungen, von international operierenden zivilgesellschaftlichen Organisationen und von Medien mit ausländischen Anteilseignern reglementieren, wenn nicht gar unterbinden? Resilienz würde dann an geschlossene Gesellschaften mit Informationsmonopol erinnern.

Die Verteidigung der offenen Gesellschaft umfasst gesetzliche Einschränkungen der Datennutzung, ein „Selbstbestimmungsrecht" über eigene Daten, d.h. keine Massenüberwachung, den Schutz von Daten beim Verkehr zwischen Diensten, den Kampf gegen rechtswidrige Inhalte, Vorkehrungen gegen Desinformation, die Integrität von Wahlen und den normativen Appell an die professionelle Integrität von Nachrichtenvermittlung durch Massenmedien, darunter sozialen Medien – möglicherweise bis hin zu deren Regulierung oder der Zertifizierung von deren Qualität. Informationen sind ein öffentliches Gut und auch eine Ware. Warum also sollte der Verbraucherschutz sich nicht auch auf die Nachrichtenvermittlung erstrecken? Resilienz könnte in der Zertifizierung von Massenmedien durch eine Art TÜV bestehen. Die Begrenzung äußerer Einflussnahme kann sich in offenen Gesellschaften nicht auf die Zensur von Informationen und Meinungen beziehen, solange diese nicht zu strafbaren Handlungen aufrufen oder dazu Vorschub leisten. Offene Gesellschaften müssen allerdings gewährleisten, dass eine sachbezogene politische Willensbildung möglich ist, und zwar durch Medien, die professionellen Standards genügen und durch Sicherstellung der Fairness von Wahlen.

4.3 Präventive und reaktive Ansätze

Unter Experten besteht ein breiter Konsens darüber, dass der Schutz politischer Prozesse und Wahlen eines ressortübergreifenden („*whole-of-government approach*") und gesamtgesellschaftlichen Vorgehens bedarf (Brattberg/Maurer 2018: 29; Herpig et al. 2018: 36f.; Cederberg 2018: 33). Dies spiegelt sich unter anderem auch im Ausbau von Cyberverteidigungsfähigkeiten und in der Gesetzgebung gegenüber Anbietern sozialer Medien wider. Die Maßnahmen sind überwiegend präventiver und reaktiver Natur und zielen darauf ab, die politische Resilienz zu erhöhen, sodass externe Einflussnahme auf politische Prozesse und Wahlen misslingt bzw. weniger Wirkung entfalten kann.

Eine Forschergruppe der „*Carnegie Cyber Policy Initative*“ empfiehlt, Wahlsysteme und -prozesse als Teil kritischer Infrastruktur zu behandeln (Brattberg/Maurer 2018: 29). Dazu müssten ausreichend Anstrengungen und Ressourcen zum Schutz vor potenzieller Einmischung durch Informations- und Kommunikationstechnologie aufgewendet werden. Einem potenziellen Kontrahenten gelte es zu vermitteln, dass er mit einer ernsthaften Antwort rechnen müsse. Herpig et al. schlagen vor, dass Regierungen öffentlich definieren, was als Wahlbeeinflussung gilt und welche Systeme dies beinhaltet. Der Schutz von Wahlen solle als Teil der nationalen Sicherheit gesehen werden (Herpig et al. 2018: 36). Eine federführende Behörde könnte mit dem Schutz von Wahlen betraut werden, und sie bedürfe eines klaren Mandats, um effektiv wirken zu können. Alle am Schutz von Wahlen beteiligten Institutionen wie Geheimdienste, Strafverfolgungsbehörden, Außen- und Innenministerien und Wahlbehörden sollten sich deshalb in einem institutionalisierten Rahmen koordinieren (Brattberg/Maurer 2018: 29; vgl. Herpig et al. 2018: 37).

Ein transparenter Umgang mit dem Schutz vor externer Einflussnahme verspricht durchaus Wirkung. Die öffentliche Warnung potenzieller Gegner, wie dies die Bundesregierung vor den Bundestagswahlen 2017 getan hat, hilft, Cyberattacken abzuschrecken, indem deutlich gemacht wird, dass mit Reaktionen zu rechnen ist (Brattberg/Maurer 2018: 30; vgl. Conley 2018: 3; Herpig et al. 2018: 36). Die Warnung der Bundesregierung, des Verfassungsschutzes und des Bundesnachrichtendienstes vor russischen Manipulationen im Vorfeld der Bundestagswahl 2017 zeigten durchaus Wirkung. So kann einerseits abgeschreckt, zugleich aber die Bevölkerung sensibilisiert werden (Brattberg/Maurer 2018: 30; Conley 2018: 3). Ebenso wichtig ist es, die Bevölkerung möglichst umfassend und stichhaltig über Cyberattacken aufzuklären (Brattberg/Maurer 2018: 31; Herpig et al. 2018: 39).

Der Ausbau von Cyberverteidigungsfähigkeiten umfasst auch die technische Resilienz. Regierungen sollten den Schutz von Wahlen als eine gemeinsame Aufgabe von Behörden, privaten und zivilgesellschaftlichen Akteuren betrachten. Dies bedeutet, alle am Schutz von Wahlen beteiligten Akteure finanziell und personell adäquat auszustatten (Herpig et al. 2018: 36). Um Wahlen vor Manipulation zu schützen, optimieren Regierungen in der Regel den Schutz der Wahlinfrastruktur. Dafür sind kontinuierlich Verletzlichkeitsanalysen nötig. Gegebenenfalls sollte man von der elektronischen Stimmabgabe und -auswertung zu Papier und Stift zurückzukehren (Brattberg/Maurer 2018: 29; Conley 2018: 3; Herpig et al. 2018: 36 f.). In den Niederlanden wurde 2017 das elektronische Wählen abgeschafft, um das Vertrauen der Wähler in die Wahl wieder zu erhöhen. Frankreich verbot nach einer Verletzlichkeitsbewertung im Jahre 2012 das ausschließlich für Wähler in den Überseeterritorien zugelassene elektronische Wählen für die Parlamentswahl im

Juni 2017 gänzlich. Man kehrte zur Papierwahl und manuellen Stimmauszählung zurück (Conley 2018: 3). Regierungen, so das Plädoyer, sollten NGOs, Parteien und Kampagnen finanziell und mit Know-how unterstützen, um deren Cybersicherheit zu stärken bzw. fortzuentwickeln (Brattberg/Maurer 2018: 30; vgl. Conley 2018: 3; Herpig et al. 2018: 39). Regierungen und Parteien sollten zudem Notfallpläne erarbeiten, die ihnen nach einem Vorfall Zeit verschaffen und Panik verhindern (Brattberg/Maurer 2018: 30; Herpig et al. 2018: 36).

Sven Herpig, Juliane Schütz und Jonathan Jones von der Stiftung Neue Verantwortung sind der Ansicht, dass es keinen vollständigen Schutz vor Diebstahl, der Veröffentlichung, Manipulation oder der Blockade von wahlrelevanten Daten geben könne. In ihrem Leitfaden „Der Schutz von Wahlen in vernetzten Gesellschaften – wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt" schreiben sie: Für „Strategien zum Schutz von Wahlen sind daher neben der Erhöhung technischer Sicherheitsstandards genauso solche Maßnahmen entscheidend, die den Schaden erfolgreicher Angriffe verringern und die Widerstandsfähigkeit der Demokratie insgesamt verbessern" (Herpig et al. 2018: 4).

Brattberg und Maurer zufolge müssen Vorkehrungen zum Schutz des Wahlprozesses institutionalisiert werden, um eine enge Koordination aller relevanten Regierungsbehörden, Geheimdienste, Strafverfolgungsbehörden, Außen- und Innenpolitik und Wahlbehörden über alle Staatsebenen hinweg zu gewährleisten. Die federführende Betrauung einer Behörde mit einem zwischenbehördlichen und „*whole-of-government approach*" habe sich als sinnvoll erwiesen (Brattberg/Maurer 2018: 29; Herpig et al. 2018: 37). Die federführende Behörde solle alle potenziellen Gefahren überwachen und in Kooperation mit den Geheimdiensten regelmäßig Gefahrenbewertungen vornehmen. Eine weitere Empfehlung zielt darauf, Angriffe so kostspielig und schwerfällig wie möglich zu machen (Brattberg/Maurer 2018: 29). Brattberg und Maurer empfehlen regelmäßige Verletzlichkeitsanalysen, beispielsweise von Wahlauswertungssoftware, um Risiken zu identifizieren. Dies würde auch die Integrität der Lieferketten von Soft- und Hardware und von staatlichen Auftragnehmern beinhalten (Brattberg/Maurer 2018: 30). Um zu gewährleisten, dass die verwendete IT dem aktuellen Stand der Technik entspricht, schlagen Herpig et al. ein „*Hack the Election*"-Programm vor, um Schwachstellen aufzudecken, die anschließend verpflichtend geschlossen werden (Herpig et al. 2018: 36 f.).

Regierungen sollten politische Parteien und Wahlkampagnen mit Expertise unterstützten, wie dies in Deutschland, Frankreich und Großbritannien bereits geschieht (Brattberg/Maurer 2018: 30; vgl. Conley 2018: 3). Regierungen können mit Partei- und

Kampagnen-Mitarbeitern zusammenarbeiten, um die Cybersicherheit und „Cyberhygiene“ zu verbessern. Herpig et al. sprechen von einer „Fähigkeitsentwicklung“, die es durch Regierungen finanziell zu fördern gelte (Herpig et al. 2018). Brattberg und Maurer zufolge müssten Parteiführungen auch Eigenverantwortung für den Schutz demokratischer Prozesse übernehmen (Brattberg/Maurer 2018: 30). Wahlkampagnen sind „weiche Ziele“ – nur wenig Zeit und Geld stehen zur Verfügung, um langfristige Sicherheitsstrategien zu entwickeln (Adkins et al. 2018: 7).

Bildungskampagnen über Desinformationsmethoden erhöhen die Resilienz ebenfalls. Die Autoren der Stiftung Neue Verantwortung empfehlen, dass Regierungen den Medien und Wählern Sicherheitsstrukturen und IT-Systeme „proaktiv“ vermitteln:

> „Das Ziel muss sein, falschen Vorstellungen zu begegnen, mit Ängsten aufzuräumen, die Transparenz zu verbessern und entgegen der Praxis ‚*Security by Obscurity*‘ (Sicherheit durch Verschleierung) regelmäßig Informationen anzubieten, etwa [...] im Rahmen des Versands von Wahlinformationen“ (Herpig et al 2018: 39).

Ein kritischer Umgang mit Offline- und Online-Medien solle Teil von Bildungsplänen werden. Schweden hat so z.B. Schulprogramme zum Erkennen von Falschnachrichten aufgelegt, neben den Medien wird auch die Bevölkerung in den Schutz von Wahlen einbezogen (Cederberg 2018: 33). Watts plädiert für einen kritischen Umgang mit Nachrichten und deren Verbreitung in sozialen Medien, letztlich sind es demnach die Bürger, die die Demokratie vor ihren Feinden schützen (Watts 2018: 154).

Grundsätzlich sollen Adkins et al. zufolge alle Wahlkampagnen eine Kultur der Informationssicherheit etablieren, ihre Daten online in einer Cloud speichern, da diese sicherer sei als alles, was eine Kampagne aufbauen könne, eine Zwei-Faktor-Authentifizierung einführen, d.h. die Kombination aus einem Passwort und einem über ein zweites Gerät generiertes Einmalpasswort, sowie verschlüsselte Chatprogramme verwenden und Notfallpläne erstellen (Adkins 2018: 12). Die Binnenkommunikation von Wahlkämpfern soll folglich vor Infiltration geschützt werden. Singer und Brooking betonen ebenfalls die Bedeutung der Medienbildung, die von Familien, Schulen und Universitäten wahrgenommen werden müsse und die es auszubauen gelte (Singer/Brooking 2018: 264). Regierungen und Geheimdienste sollten darüber hinaus Informationen, wenn möglich auch forensische Beweise, über Cyberoperationen publik machen, um die öffentliche Sensibilität zu stärken und Informiertheit zu demonstrieren.

Der traditionelle Journalismus leidet derweil unter einer Vertrauenskrise, relevante Teile der Bevölkerung halten den klassischen Medien Manipulation, Voreingenommenheit und Arroganz vor – das Einfallstor für Medien à la *Russia Today*, Sputnik oder deutschsprachigen Transmissionsriemen wie den sogenannten „Nachdenkseiten", die sich dann als Anbieter „unterdrückter Informationen" präsentieren.[9] Eine Rückkehr zur hegemonialen Stellung öffentlich-rechtlicher Medien wäre freilich anachronistisch und irreal. Die Nachrichtenlandschaft hat sich unwiederbringlich ausdifferenziert – neben Fernsehen, Radio und Printmedien werden eine Fülle von Nachrichten online rezipiert. Die konventionelle Rollenverteilung zwischen Informationsanbietern und Informationsempfängern löst sich tendenziell auf. Gegen den Vorwurf, dass „Mainstream"-Medien nicht objektiv berichteten, kann indes nur qualitativ hochwertiger Journalismus helfen, der umfangreich und sachlich korrekt informiert – er ist Voraussetzung für eine funktionsfähige Demokratie. In Bezug auf die Verbreitung oder Weiterverbreitung von Falsch- und Desinformationen ist die Selbstverantwortung der Nutzer sozialer Medien elementar. Dabei können Bildungsmaßnahmen und Sensibilisierungskampagnen die Wehrhaftigkeit der Demokratie stärken.

Mittlerweile gibt es eine Reihe Plattformen, die sich der Aufdeckung von Desinformation widmen. Ein Beispiel ist die Organisation „Stopfake.org". Angehende ukrainische Journalisten und Redakteure befassen sich im Kontext des Ukrainekonflikts seit fünf Jahren mit der Aufdeckung von russischen Falschnachrichten, insbesondere den wiederkehrenden Mustern visueller und narrativer Fake-Produktion. StopFake ist zu einer Autorität bei der Aufdeckung russischer Medienpraktiken geworden und trägt zur politischen Bildung nicht unwesentlich bei – Nutzer können Mechanismen der Fälschung schneller erkennen.[10] Die meisten Maßnahmen zur Steigerung politischer Resilienz zielen auf bessere internationale Kooperation, den Ausbau von Cyberverteidigungsfähigkeiten und die Einbindung der breiteren Öffentlichkeit.

Um der Lancierung von Falsch- und Desinformationen oder extrem einseitiger, politisch-plakativer Berichterstattung entgegenzutreten, ist es sinnvoll, durch einen Medienrat aus Regierungs- und Medienvertretern Standards zu formulieren und darüber Rechtfertigungszwänge zu schaffen. Selbstverpflichtungen von Medienanbietern und die Stärkung journalistischer Qualitätsstandards dürften letztlich wirksamer sein als gesetzliche Einschränkungen. Regierungen können auf die Anbieter sozialer Medien einwirken, Mecha-

[9] http://heute-morgen-uebermorgen.digital/blog/snowball/wenn-politik-journalismus-macht/.
[10] https://www.stopfake.org/de/start/.

nismen der Faktenprüfung einzuführen (Brattberg/Maurer 2018: 31; Herpig et al. 2018: 38). Ein Medienrat auch für nicht-öffentlich-rechtliche Medien könnte Leitlinien für die digitale Ethik annehmen und so dem Platzieren von Falschnachrichten vorbeugen. Regierungen können Medienvertreter dazu animieren, ihre Qualitätsstandards zu erhöhen und Maßnahmen gegen die Verbreitung von Falschnachrichten im Journalismus zu ergreifen. Anbieter sozialer Medien sollten zudem befähigt werden, Desinformation zu identifizieren und deren Verbreitung zu minimieren. Falsche Accounts sollten blockiert und gefälschte Inhalte markiert werden. Bei Gesetzesvorhaben – z.B. in Bezug auf das Entfernen illegaler Inhalte, Konsequenzen für die Erstellung, Verbreitung und Verstärkung von Falschinformationen oder Transparenzanforderungen an politische Werbung – ist es ratsam, Medienvertreter und zivilgesellschaftliche Gruppen einzubinden, um eine erfolgreiche Implementation zu ermöglichen.

Brattberg und Maurer empfehlen einen regelmäßigen und institutionalisierten Austausch – vor allem im Vorfeld von Wahlen – von „Lessons Learned" und „Best-Practices" zwischen Regierungen demokratischer Staaten. Foren hierfür könnten der Europäische Auswärtige Dienst mit der „*East-Strat-Com Task Force*", das „*NATO-StratCom Communications Center of Excellence*" oder das finnische „*Center of Excellence on Countering Hybrid Threats*" sein. Herpig et al. empfehlen schließlich, dass der Wahlausgang durch transparente und sichere Audits nachvollziehbar gemacht wird (Herpig et al. 2018: 38).

Heather A. Conley hat die französischen Präsidentschaftswahlen im Mai 2017 als ein erfolgreiches Beispiel zur Abwehr russischer Wahlbeeinflussung untersucht. So sei Frankreich nicht wie die USA mit der Fehlannahme in die Wahlen gegangen, dass russische Wahlbeeinflussung qua Desinformation nicht funktionieren könne, vielmehr hätte Frankreich die Erfahrungen anderer europäischer Länder mit russischer Wahlbeeinflussung ausgewertet. Die französische Regierung habe sich im Unterschied zur amerikanischen Administration nicht gescheut, bei den Macron-Leaks zu intervenieren. Sie habe dadurch gezeigt, dass eine Regierung auch unabhängig und unpolitisch eingreifen kann (Conley 2018: 2ff., auch zum folgenden). Ebenso sei deutlich geworden, dass sich politischer und öffentlicher Druck auf Anbieter sozialer Medien lohne, um diese dazu zu bewegen, Maßnahmen gegen Desinformation zu ergreifen. So habe Facebook in Frankreich vor der Wahl 70.000 unechte Accounts gelöscht, was das Unternehmen zuvor noch nie getan hatte. Die Entscheidung der Macron-Kampagne und des späteren Präsidenten Macron, den russischen Sender RT und Sputnik aufgrund der systematischen Verbreitung von Falschinformationen die Akkreditierung für Pressekonferenzen zu entziehen, war zwar umstritten und nährte das russische Narrativ, wonach Frankreich genau das mache, wofür es Russ-

land kritisiere. Die Teilnahme an Pressekonferenzen war allerdings grundsätzlich nur nach Einladung möglich. RT und Sputnik wurden als Propagandaeinrichtungen, nicht als Medienagenturen behandelt.

4.4 Offensive Gegenmaßnahmen?

Der ehemalige FBI-Agent und Fellow am *Center for Cyber and Homeland Securiy* der George Washington University, Clint Watts, sieht das Ziel russischer Kampagnen im Zerfall der EU und der NATO, der Verbreitung von Nationalismus und der Unterminierung der Demokratie, er plädiert für eine offensive Reaktion auf das russische Vorgehen. Amerikas auf *soft power* basierende Gegenmacht würde allerdings darunter leiden, dass der Anti-EU- und Anti-NATO-Tenor selbst von der Regierung unter Donald Trump bedient würde (Watts 2018: 193). Während Russland die gesamte Bandbreite sozialer und konventioneller Medien für seine Propaganda ohne rechtliche und bürokratische Grenzen nutze, litten die Informationsoperationen der USA unter strukturellen Mängeln. So habe es während des Kalten Kriegs die *U.S. Information Agency* (USIA) gegeben, die öffentliche Diplomatie mit der Mission betrieben habe *„‚to understand, inform and influence foreign publics in promotion of the national interest, and to broaden the dialogue between Americans and U.S. institutions, and their counterparts abroad'"*. Das bestehende System aus US-Beamten und privaten Auftragnehmern, die „Gegenpropaganda" durchführten, sei aufgrund von überbordender Bürokratie unflexibel und verglichen mit den russischen Methoden der *Internet Research Agency* ineffektiv (Watts 2018: 201 und 207ff.).

Singer und Brooking erinnern wehmütig an die *Active Measures Working Group*, die US-Regierungsbeamte, Geheimdienstmitarbeiter, Diplomaten, Pädagogen und Journalisten während des Kalten Krieges vereinte, um Falschmeldungen des KGB entgegen zu treten, heute gäbe es kein Äquivalent dazu (Singer/Brooking 2018: 263). Doch Watts zufolge sollten das *Department of Homeland Security* und das US-Außenministerium öffentliche Stellungnahmen zu Falschmeldungen über die amerikanische Innen- und Außenpolitik veröffentlichen, das FBI solle wiederum bei der Untersuchung von Hacks antizipieren, welche Ansatzpunkte es für potenzielle Einflussnahme gäbe.[11] Das Verteidigungsministerium und die Geheimdienste sollten ein System zum Aufspüren von russischen Desinformationskampagnen in sozialen Medien entwickeln. Darüber hinaus müsse der Westen kollektiv entscheiden, wie er auf das russische Vorgehen unter Putin reagiere. Allerdings empfiehlt er nicht, sich in russische Wahlen ähnlich manipulativ einzumischen, wie es Russland im Westen tue (Watts 2018: 209).

[11] *„Anticipating rather than reacting to kompromat can help inoculate the victim from negative influence"* (Watts 2018: 209).

Um Gegenmaßnahmen zu ergreifen ist es Rid und Buchanan zufolge vonnöten, den Handlungsbedarf überhaupt erst einmal anzuerkennen. In den USA ignorierten jedoch große Teile der politischen Öffentlichkeit die „neuen Bedrohungen". Für Rid und Buchanan ist die Verletzlichkeit von Demokratien gegenüber Cyber- und Einflussoperationen auch eine Folge des laxen Umgangs mit der Cybersicherheit: „*Facts are too often poorly shared, major incidents not revealed, with too many public commentators still struggling to distinguish firm forensics from flimsy*" (Rid/Buchanan 2018: 4).

Die Wissenschaft würde auf dem Feld der Cybersicherheit wiederum „nicht liefern"; 25 Jahre nach den ersten bahnbrechenden Werken seien Kernkonzepte immer noch nicht ausreichend fundiert, das Defizit unterminiere die Demokratie selbst (Rid/Buchanan 2018: 4). Die Politik habe nicht mit der vor allem seit 2013 gestiegenen Anzahl an Vorfällen mitgehalten. So gäbe es eine Vielzahl an Fachkonferenzen, die Zahl der Graduiertenstudiengänge in Cybersicherheit nähme zu. Große Medienkonzerne hätten mittlerweile Reporter für die Berichterstattung über Cybersicherheit, wodurch sich die öffentliche Berichterstattung signifikant verbessert habe, gleichzeitig stagniere jedoch die Forschung auf dem Feld der Cybersicherheit (Rid/Buchanan 2018: 7).

Eine Option bestünde darin, mit robusten Maßnahmen auf Cybersubversion zu reagieren. So sieht die *Presidential Policy Directive 20* der USA sogenannte *Defensive Cyber Effects Operations* zur Verteidigung oder dem Schutz vor unmittelbaren Gefahren oder akuten Attacken vor (in Federation of American Scientists o.A.: 3). Solche Operationen müssen nicht zwangsläufig in den Netzwerken des Urhebers durchgeführt werden, sondern können sich auf die Infrastruktur des Internets beschränken (Buchanan 2017: 183). So blockierte das US-Cyberkommando im Kontext der US-Zwischenwahlen zum Kongress im November 2018 den Internetzugang der *Internet Research Agency*, die in den USA u.a. während des Präsidentschaftswahlkampfes 2016 Zwietracht in sozialen Medien säte (Nakashima 2019).

Der Nutzen von Gegenoperationen ist indes fraglich, da subversive Aktivitäten nicht auf einen Tag beschränkt sind. Einflusskampagnen ausländischer Mächte wären ohnehin erfolglos, wenn sie nicht Ansatzpunkte finden würden, etwa in der Führungsschwäche einer Regierung oder der Identitätskrise eines Landes, wodurch die Verteidigung demokratischer Werte erschwert wird (Watts 2018). Erfolge russischer Operationen liegen in der abnehmenden Attraktivität eines Landes oder einer internationalen Organisation begründet, die damit anfälliger für Propaganda werden.

Gegenoperationen entfalten am ehesten symbolische Wirkung, sie erhöhen die Kosten für den Urheber und signalisieren die eigenen Fähigkeiten und die eigene Entschlossenheit. Bereits im Vorfeld einer Zwischenwahl zum US-Kongress versendete das US-Cyberkommando gezielt Nachrichten an russische Regierungs- und Nicht-Regierungsakteure und signalisierte diesen, dass ihre Identität bekannt ist und sie im Falle von Wahlbeeinflussungen öffentlich angeklagt sowie mit Sanktionen belegt werden könnten (Barnes 2018).

Eine Verständigung über übergreifende, international gültige Normen des Verhaltens im Cyberraum steht erst am Anfang, die Möglichkeiten und Grenzen einer diskursiven Verständigung sind bisher nicht ausgeleuchtet. Eine Vielzahl von Initiativen, Teil derer auch die Außenkulturpolitik ist, möchte dazu beitragen, das Internet als Raum der Freiheit, der Ertüchtigung von Zivilgesellschaft, des Multilateralismus sowie der Entwicklung zu bewahren.

Die Initiative der *World Wide Web Foundation* für einen Vertrag über das Netz (*contract for the web*) wurde bereits von 8.000 Institutionen und Personen unterzeichnet. Regierungen sollen demnach sicherstellen, dass sich jeder Mensch mit dem Internet verbinden kann und das Grundrecht auf Schutz der Privatsphäre respektiert wird. Das Web solle eine globale öffentliche Ressource bleiben.[12] Andere Autoren plädieren für einen „digitalen Friedensplan", um ein Wettrüsten im Cyberspace einzugrenzen, insbesondere um autonome Waffensysteme zu regulieren (Dahlmann/Dickow 2019). Firmen aus dem elektronischen Business zeigen sich wiederum zunehmend beunruhigt, dass Staaten Internet-Unternehmen angreifen könnten. Vertreter von Microsoft befürchten, dass Staaten Technologiefirmen, den Privatsektor oder kritische Infrastrukturen angreifen. Statt technische Schwachstellen zu nutzen, sollten sie die Hersteller darüber informieren. Cyberwaffen sollten wiederum begrenzt und präzise in ihrer Wirkung sein – nicht wie die Malware WannaCry oder NotPetya, die Milliardenschäden angerichtet hatten. Im April 2018 unterzeichneten 34 Firmen den *Cybersecurity Tech Accord*, indem sie sich verpflichteten, Regierungen bei Angriffen auf unschuldige Bürgerinnen und Bürger oder Firmen nicht zu unterstützen. Der französische Präsident Emmanuel Macron initiierte 2018 zudem den *Paris Call for Trust and Security in Cyberspace*, dem sich alle 28 EU-Staaten, 27 der 29 NATO-Mitglieder und Firmen wie Microsoft, Google, Facebook, Intel und Finanzdienstleister wie Citigroup und Visa anschlossen und böswillige Cyberaktivitäten in Friedenszeiten verur-

[12] https://contractfortheweb.org/about/.

teilten, welche signifikanten, unterschiedslosen oder systemischen Schaden für Individuen und kritische Infrastrukturen verursachen können (Ranger 2018).

Die Europäische Datenschutz-Grundverordnung (DS-GVO), die als Ergebnis von langwierigen Verhandlungen und Kompromissen zustande kam und am 25.5.2016 vom Europäischen Parlament angenommen wurde, reagiert schließlich auf Fragen, die durch „Big Data" und neue Techniken oder Arten der Datenverarbeitung wie Profilbildung, Webtracking und dem Cloud Computing für den Schutz der Privatsphäre aufgeworfen wurden.[13] Ziel der DS-GVO ist eine Balance zwischen Wirtschafts- und Verbraucherinteressen, indem das Grundrecht auf informationelle Selbstbestimmung durch höhere Transparenz und mehr Mitbestimmung der Bürgerinnen und Bürger gestärkt wird. Gleichzeitig schafft sie einen Rechtsrahmen für datenverarbeitende Unternehmen und innovative Geschäftsmodelle. Die DS-GVO schafft ein europaweit einheitliches Datenschutzniveau. Wettbewerbsverzerrungen und Marktzugangsbarrieren infolge unterschiedlicher nationaler Datenschutzbestimmungen werden beseitigt. Die DS-GVO setzt Anreize für die „Pseudonymisierung" von Daten, d.h. der Name oder ein anderes Identifikationsmerkmal wird durch ein Pseudonym – zumeist eine mehrstellige Buchstaben- oder Zahlenkombination – ersetzt. Das macht es wesentlich schwerer, betroffene Personen zu identifizieren. Durch Pseudonymisierung können große Datenmengen ohne Personenbezug und grundrechtsschonend verarbeitet werden.

Die DS-GVO schützt die Privatsphäre von Nutzerinnen und Nutzern bei „Big Data", Webtracking und Profilbildung und definiert das „Recht auf Vergessenwerden" und auf Datenportabilität. Das sogenannte „Marktortprinzip" sorgt dafür, dass die DS-GVO Anwendung auf Datenverarbeiter findet, die nicht in der Europäischen Union niedergelassen sind, wenn eine Datenverarbeitung dazu dient, in der Europäischen Union ansässigen Personen Waren oder Dienstleistungen anzubieten. Die DS-GVO erhöht die Transparenzpflichten von Unternehmen gegenüber ihren Kunden und erweitert die Rechte der Betroffenen, so das Recht auf Auskunft: Betroffene müssen wissen, was mit ihren Daten geschieht und zu welchen Zwecken die Daten verarbeitet werden.

Unter dem Stichwort „Digitaler Marshall-Plan" optiert der Publizist Sascha Lobo für eine radikale Modernisierung der digitalen Infrastruktur, einen digitalen Investitionsfonds, ein Grundrecht auf Netzzugang, eine Art TÜV für die Löschung von Inhalten auf

[13] vgl. https://dsgvo-gesetz.de/ sowie https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung. Die folgende Passage paraphrasiert die Ausführungen der DS-GVO ohne Anspruch auf eigene Bewertung.

Social-Media-Plattformen (anstelle des „Netzwerkdurchsetzungsgesetzes“) und verpflichtende Digitalschulungen. Schließlich solle ein „Datenbundesamt“ die kostenfreie, öffentliche Zugänglichkeit staatlicher und behördlicher Daten sicherstellen. Lobo fordert eine verbraucherorientierte Digitalschutz-Taskforce, die wirksame Sanktionen gegen Online-Betrug und die Nichteinhaltung von Produktversprechen ermöglicht (Lobo 2017).

Das von den Vereinten Nationen organisierte *Internet Governance Forum* (IGF) trifft sich jährlich und versteht sich als Diskussionsplattform, auf der technische, wirtschaftliche, administrative und sicherheitspolitische Fragen der Digitalisierung sowie soziale Themen wie die digitale Gleichberechtigung und die Teilhabe sowie ein verbesserter Zugang zum Internet, schließlich der Konnex von „Internet und Menschenrechte“ diskutiert werden. Die Vertreter von 174 Staaten einigten sich darauf, im Konflikt zwischen den USA und anderen Staaten über die Verwaltung des Internets die Verantwortung des Domain Name Systems nicht anzutasten, die durch die amerikanische *Internet Corporation for Assigned Names and Numbers* unter Aufsicht des amerikanischen Handelsministerium wahrgenommen wird. Das IGF soll als Diskussionsplattform für Fragen der Bekämpfung von Spam und Cybercrime oder auch einer Neuregelung des Systems der Interconnection-Entgelte dienen. Typische Themen des IGF sind die Prävention von Jugendgewalt und Radikalisierung über das Internet, künstliche Intelligenz und Menschenrechte oder Messkriterien für ein freies, offenes, rechtsstaatliches und inklusives Internet.

Das *UN High-Level Panel on Digital Cooperation*, vom UN-Generalsekretär António Guterres am 12.7.2018 eingerichtet, sprach einige generelle Empfehlungen aus. Soziale Medien sollten sich der Gefahren für die Menschenrechte bewusst werden, Entscheidungen über Leben und Tod dürften nicht an Maschinen delegiert werden. Das UN Panel regt eine globale Verpflichtung zu digitalem Vertrauen und digitaler Sicherheit an.[14] Jeder Erwachsene soll einen bezahlbaren Zugang zu digitalen Netzen bekommen, Regierungen sollen wiederum regionale und globale *help desks* aufbauen, um die sozialen und wirtschaftlichen Auswirkungen digitaler Technologien besser zu verstehen. Das IGF und das UN High Panel sind in ihrem gegenwärtigen Format allerdings nicht dazu angetan, der Cybersubversion zu begegnen, der Fokus liegt auf der Nutzung digitaler Technologien für die Erreichung der Nachhaltigkeitsziele.

[14] https://dig.watch/processes/hlp.

Jenseits der EU-Datenschutzgrundverordnung sind die Kooperationsmöglichkeiten der EU-Mitgliedsstaaten bei weitem nicht ausgeschöpft. Sie könnten sich darauf verständigen, keine Wahlmanipulationen (durch soziale Netzwerke oder Angriffe auf die Wahlinfrastruktur) untereinander zu betreiben oder durch Dritte zuzulassen. Wahlen würden weiterhin im nationalen Raum stattfinden (bei EU-Wahlen im EU-Raum), die Mitglieder würden sich wechselseitig vor manipulativen Beeinflussungen durch externe Mächte schützen. Eine weitere Möglichkeit bestünde darin, gemeinsame Zertifizierungsstandards für soziale Netzwerke aufzusetzen – diese können sich auf das Löschen von Beiträgen, den Datenschutz, Hassreden oder technische Sicherheitsstandards beziehen. Wenn Betreiber von sozialen Netzwerken diese Sicherheitsstandards nicht einhalten, könnte es europaweite Warnungen geben. EU-Staaten könnten gemeinsam gegen Troll-Fabriken vorgehen und europaweit Bots blockieren, wenn mit ihnen die Fiktion einer Massenreaktion im Internet auf bestimmte Meldungen lanciert werden soll. In Bezug auf den Datenschutz, insbesondere die Nutzung von Daten durch politische Parteien während Wahlkämpfen, lassen sich ebenfalls Standards entwickeln. Im Raum der EU könnten bestimmte Server blockiert werden, die sich an geltende Standards nicht halten, dies hätte eine abschreckende Wirkung.

Bisher haben die Geheimdienste führender westlicher und nicht-westlicher Staaten existierende Schwachstellen in Betriebssystemen oder Netzen für die eigene Informationsbeschaffung ausgenutzt. Die Geheimdienste könnten darauf verpflichtet werden, mit dieser Art „Politik“ aufzuhören, weil das Vertrauen der Bürgerinnen und Bürger in den Staat unterminiert wird, wenn Geheimdienste sich derselben Methoden wie kriminelle Hacker bedienen. Die EU könnte dem Beispiel der USA unter der Obama-Administration folgen, diese hatte einen *Vulnerabilities Equities Policy Process* (VEP) erarbeitet (Newman 2017), um die *„risks of dissemination, the potential benefits of government use of the vulnerabilities, and the risks and benefits of all options in between“* abzuwägen und zu entscheiden, ob Informationen über eine Schwachstelle an die Softwarehersteller gemeldet oder dieses Wissen zeitweise von Militärs, Geheimdiensten oder Strafverfolgungsbehörden operativ genutzt wird (The Whitehouse 2017: 1). Eine Einigung der EU-Mitgliedsstaaten auf ein europaweites Schwachstellenmanagement, das die Nutzung von Schwachstellen, die die Mitgliedsstaaten gefunden haben, auf für die nationale Sicherheit bedeutende Fälle temporär begrenzt (vgl. Herpig 2018), könnte ein Signal an andere Staaten sein: EU-Staaten würden kurzfristige Geheimdienstgewinne zu Gunsten längerfristigen Vertrauens hintanstellen. EU-Staaten stünden weniger im Verdacht, Verursacher bestimmter Cyberoperationen zu sein (Buchanan 2017: 174). Würde dieses Signal von anderen Staaten reziprok beantwortet, ließe sich die Cybersicherheit aller Akteure erhöhen (Buchanan 2017: 170).

Wenn ein Staat sich an „patriotischem Hacking“ beteiligt, werden andere diesem Muster folgen, mit einer Aktions-Reaktions-Spirale als Folge. Wie bei konventioneller Spionage, die völkerrechtlich nicht geregelt ist (vgl. Demarest 1996, 337 f.; Buchan 2016, 20 f.), „hacken“ heute wohl schon alle Staaten. Das Verhalten ruft das klassische Sicherheitsdilemma hervor: Aus Misstrauen generierte Handlungen heizen weiteres Misstrauen an und ziehen eine sich selbst erfüllende Prophezeiung nach sich (Buchanan 2017). Es könnte freilich im Interesse von Staaten liegen, unabhängig vom politischen Regime, gegenüber der Entwicklung von Cyber-Kapazitäten von nicht-staatlichen Akteuren zusammen zu wirken, etwa gegenüber al-Qaida, der Hisbollah, der Hamas, den Zapatistas oder auch „patriotischen“ Hackern, die sich politischer Kontrolle durch ihre Patrone entziehen.

Maßnahmen zum Ausbau der Grundlagensicherheit, die Vertiefung von bilateralem Vertrauen, Beiträge zur systemweiten Sicherheit wie dem Umgang mit Schwachstellen und die Herausbildung einer Cybersicherheitsdoktrin reduzieren Fehlwahrnehmungen und minimieren damit das Cybersicherheitsdilemma. Staaten könnten sich für „neutral“ erklären, d.h. Datenflüsse über ihre Server unterbinden, die für Cyberangriffe genutzt werden. Einige Angriffsziele, z.B. auf Krankenhäuser, lassen sich als „perfide“ deklarieren. Staaten sollten nicht die kritische Infrastruktur und die Computer Emergency Response Teams anderer Staaten ins Visier nehmen und sich gegenseitig bei der Aufklärung von Cybervorfällen unterstützen. Böswillige Codes, die auf öffentliche Websites platziert werden, oder die Implantierung von *logic bombs* in die Hardware von Geräten, die weit über das intendierte Ziel hinaus Schaden anrichten, lassen sich als unterschiedslose Waffe, vergleichbar einer Chemiewaffe, diskreditieren.

„Unterschiedslosigkeit“ ist ein Problem aller bisherigen Cyberoperationen (z.B. NotPetya oder Stuxnet) und erklärt, warum eine normative oder rechtliche Einhegung schwer fällt. Cyberattacken, inklusive Cyberkriminalität, die hochstandardisierte Systeme ausnutzen, tendieren dazu, breit zu streuen. Gezielte (also nicht unterschiedslose) Cyberoperationen müssten hingegen so programmiert sein, dass sie „diskriminieren“, d.h. der Kollateralschaden kontrolliert werden kann. Das grundsätzliche Problem besteht darin, dass der Schaden von Cyberoperationen, verglichen mit militärischen Akten, bisher so subtil ist, etwa die Zerstörungswirkung, dass eine Verrechtlichung und Normensetzung schwer vorstellbar ist.

Solange der Schaden nicht massiv ist, werden sich Staaten die Option einer Cyberoperation deshalb kaum nehmen lassen. Am ehesten lassen sich rote Linien aufzeigen. Der Grundsatz der militärischen Notwendigkeit oder der Verhältnismäßigkeit im Kriegsvöl-

kerrecht lässt sich auch auf Cyberangriffe anwenden: Zu fragen wäre: Sind zivile Ziele überproportional betroffen, folglich illegitim? (Hughes 2010) Eine Lösung könnte sein, dass nur Cyberoperationen, die die Schwelle zu einem bewaffneten militärischen Konflikt überschreiten, auch militärisch beantwortet werden dürfen.

Autoritäre Staaten wie China und Russland stehen vor der Wahl, ob sie das ganze Repertoire an Angriffs- und Kontrolloptionen vorhalten wollen, denn konfrontatives Verhalten ist auf Dauer teuer und hat potenziell geschäftsschädigende Auswirkungen. Die USA haben so Mitte Mai 2019 die chinesische Firma Huawei wegen Spionage auf eine Sanktionsliste gesetzt und gefordert, dass es vom Ausbau des 5G-Netzes ausgeschlossen wird. Wirkung zeigten die Sanktionsdrohungen gegen Huawei schon vorab: Der Konzern erklärte sich bereit, mit einzelnen Ländern No-Spy-Abkommen abzuschließen.[15] Es ist noch zu früh zu bestimmen, ob Staaten wie die USA, China und Russland bereit sind, einen internationalen Cyber-Vertrag abzuschließen oder zunächst ihre Kapazitäten noch weiter ausbauen wollen (Abebe 2016).

Chancen für Übereinkünfte bestehen im Austausch von Informationen bei geteilten Gefahren, angesichts von *Zero-Day-Exploit-Attacks*[16] oder in Gestalt von Unterstützungsabkommen bzw. Unterstützungsmechanismen. Kooperation ist auch denkbar bei der Einhegung des Dual-Use-Charakters von Sicherheitssoftware oder der Entwicklung und Verwendung von Software, mit der Schwachstellen aufgedeckt und ausgenutzt werden, um die eigene Netzwerksicherheit zu verbessern (Buchanan 2017: 167f.). Bisher ungelöst ist das Problem der Verifikation von Attacken durch nicht-staatliche Akteure – Staaten werden sie nie gänzlich kontrollieren können, zugleich nutzen sie solche Hacker, weil sich derart die eigene Verantwortung abstreiten lässt.

Mit Ländern wie China, Russland oder Iran sollten Gespräche geführt werden, um digitale Mindestnormen anzustreben und im Bereich der „digitalen Kriegsführung" Tabus zu errichten – vergleichbar jenen der atomaren Rüstungskontrolle. Staaten können gegenüber anderen Staaten signalisieren, wie sie mit Cyberoperationen umgehen, d.h. mit welchen Konsequenzen reagiert würde und welches Verhalten als inadäquat oder uner-

[15] https://www.zeit.de/wirtschaft/unternehmen/2019-05/spionagevorwuerfe-usa-huawei-schwarze-liste-donald-trump.

[16] Ein Zero-Day-Exploit ist eine dem Softwarehersteller, dem Nutzer und der Öffentlichkeit unbekannte Schwachstelle, d.h. es besteht für Entwickler „Null Tage Zeit", die entsprechende Schwachstelle zu beheben, wohingegen der Angreifer sie unmittelbar für eine Cyberoperation nutzen kann und somit mit hoher Wahrscheinlichkeit erfolgreich ist. Das Auffinden von Zero-Day-Exploits und die Entwicklung von Programmen zu deren Ausnutzung ist zeitintensiv und erfordert ein hohes Maß an Expertise.

wünscht angesehen wird, um Fehlwahrnehmungen zu reduzieren. Das Annoncieren von roten Linien kann längerfristig zu einer Verhaltensänderung führen. Ansatzpunkt kann *Cross-Domain-Deterrence* sein („*the use of threats of one type, or some combination of different types, to dissuade a target from taking actions of another type to attempt to change the status quo*" (Gartzke/Lindsay 2019: 4). Es handelt sich dabei um Wirtschaftssanktionen, diplomatische Maßnahmen oder juristische Anklageerhebungen (Lindsay/Gartzke 2019; Buchanan 2017: 183).

Ein ungehinderter Rüstungswettlauf im Cyberraum dürfte kaum im Interesse der Staatengemeinschaft liegen, auch wenn kurzfristige Nutzenkalküle gegenüber dem kollektiven Schaden dominieren. Länder, die über erhebliche Cyber-Kapazitäten verfügen, sollten sich sukzessive über Möglichkeiten der Rüstungskontrolle im Cyberraum verständigen, z.B. dass Satelliten nicht angriffen werden oder keine Hacker-Angriffe gegeneinander unterstützt oder geduldet werden. Rüstungskontrolle bleibt allerdings schwierig aufgrund des Dual-Use-Charakters von Cybertechnologien und der Ununterscheidbarkeit offensiver von defensiven Cyberfähigkeiten. Mischa Hansel resümiert:

> „Es mangelt also nicht an öffentlich verfügbarer Expertise. Hingegen fehlt eine gemeinsame politische Vision für die internationalen Beziehungen im Cyberspace. Militärs, IT-Sicherheitsfirmen und bürgerrechtliche engagierte Forschungsinstitute vertreten dezidiert unterschiedliche politische Werte […] Auch gibt es noch keine starke und institutionalisierte Lobby für vertrauensbildende Maßnahmen im Cyberspace, geschweige denn eine transnational organisierte Rüstungskontrollgemeinde. Die transnationale Verständigung über Fragen der Cybersicherheit geht in überaus kleinen Schritten voran. Ob die Differenzen zwischen unterschiedlichen Expertennetzwerken schrittweise weiter abgebaut werden können oder im Zeichen eines ‚cyber-militärisch-industriellen Komplexes' sogar noch zunehmen werden, bleibt vorerst eine offene Frage" (Hansel 2013: 301f).

5. Zusammenfassung und Ausblick

- Die Normenentwicklung im Cyberraum steht erst am Anfang. Pessimistische Beobachter sehen nur Anarchie und nationale, egoistische Interessen, einen Krieg aller gegen alle, der in ein „Splinternet", d.h. den Zerfall des Internet in diverse Teilnetze münden wird. Die quasi-monopolistische Stellung der USA im Cyberraum gehört definitiv der Vergangenheit an. Doch ob Oligopole entstehen, d.h. neben dem amerikanischen ein chinesisch-dominiertes und ein europäisches Internet sich parallel zueinander behaupten, ist noch nicht ausgemacht. Weniger fatalistische Beobachter halten die Entstehung von Normen zumindest für distinkte Bereiche des Cyberraums für möglich – die Kosten einer Fragmentierung und Segmentierung des Internet wären extrem hoch.
- Die Studie plädiert dafür, dass offene, demokratische Gesellschaften ihre Wehrhaftigkeit stärken, um die Integrität von Wahlen und die Qualität von Nachrichten als Grundlage aufgeklärter Meinungs- und Willensbildung zu schützen. Resilienz kann als kulturelle Praxis verstanden werden; nur eine lebendige demokratische Kultur „widersteht" autoritären Versuchungen. Die Resilienz von Demokratien gegen Subversion kann nur im Vertrauen in die Demokratie selbst bestehen, d.h. der Verteidigung von prozessualer Fairness, dem Wettbewerb, der Rechenschaftspflicht und der Ergebnisoffenheit von politischen Auswahlprozessen. Es gilt, Wahlen als Kern der Demokratie zu schützen, und zwar als Teil der kritischen Infrastruktur. Meinungen, und seien sie selbst von ausländischen Mächten gesponsert, gehören zum legitimen Diskurs, außer sie rufen zu Straftaten auf oder bedrohen den inneren Frieden. Es darf keine Zensur geben oder eine Rückkehr zum McCarthyismus während der Hochphase des Kalten Krieges.
- Gesellschaften und Gesellschaftsschichten müssen durch Bildung und Digital Literacy gegen Subversion gewappnet werden. Zudem sollte eine plurale Medienlandschaft einschließlich der Förderung von Qualitätsjournalismus und investigativem Journalismus unterstützt werden. Weltweit sollte verstanden werden, wie Desinformation funktioniert. Aktive Kommunikationsmaßnahmen von Seiten der Auswärtigen Kultur- und Bildungspolitik gegenüber verletzlichen Bevölkerungsgruppen sollten verstärkt werden (vgl. Meister 2018).
- Es gilt, professionelle Medienstandards zu wahren, die Projekte zur Medienkompetenz und digitale Kommunikation als Thema in der Auswärtigen Kultur- und Bildungspolitik zu fördern, gegen Hassrhetorik auch mit rechtlichen Mitteln vorzugehen und massenmanipulative Bots in sozialen Medien oder im E-Mail-Verkehr zu blockieren. Soziale Medien können aufgefordert werden, gewaltverherrlichende Inhalte und

absichtsvoll verbreitete Falschnachrichten zu blockieren oder falsche Accounts zu löschen. Ein Medienrat könnte professionelle und ethische Standards der Datenerhebung und der Berichterstattung auch für soziale Medien setzen und damit Beurteilungskriterien bereitstellen. Professionelle Standards der Berichterstattung gilt es gegenüber Manipulation, Desinformation und Versuchen der gesellschaftlichen Polarisierung zu verteidigen, und zwar mit Hilfe von Aufsichtsgremien, Transparenzregeln und Auflagen zur Löschung von rechtswidrigen oder strafbaren Inhalten.

- Zwischen Staaten mit unterschiedlichen politischen Regimen sind vertrauensbildende Maßnahmen gefordert, die illegitimes Verhalten im Cyberraum definieren. Als Ausgangsbasis hierfür können Projekte dienen, die das gegenseitige Verständnis der Wahrnehmungen und Diskurse von Sicherheit und Gefährdungslagen fördern. Chancen für Übereinkünfte bestehen im Austausch von Informationen bei geteilten Gefahren oder bei gegenseitiger Unterstützung im Falle von Cyberattacken. Unabhängig vom jeweiligen politischen Regime können Normen für den Umgang mit Cyberkriminalität aufgestellt werden.
- Staaten können Wissen über *Zero-Day-Exploits* teilen, anstelle sie für Cyberoperationen zu nutzen. Denkbar sind gemeinsame Reaktionen auf Cyberangriffe, die Vereinheitlichung von Sicherheitsstandards, die Blockade von Servern, die diese Standards nicht einhalten, oder die gemeinsame Reaktion auf Cyberattacken von Akteuren wie ISIS, al-Qaida oder anderen Terrorgruppen. Bestimmte Mittel und Ziele könnten für unangemessen erklärt werden, z.B. Angriffe auf Krankenhäuser, Atomkraftwerke oder Elektrizitätsnetze. Das Platzieren von schädlicher Software auf öffentlichen Webseiten oder von *logical bombs* könnte ebenfalls zum Tabu erklärt werden. Schließlich können Regeln der Angemessenheit, die im Kriegsrecht gelten, auch auf Cyberangriffe übertragen werden: Nur Angriffe, die in ihrer physischen Zerstörungswirkung vergleichbar einem Krieg sind, würden militärische Reaktionen rechtfertigen.
- Die Kooperation sollte auf europäischer Ebene beginnen. So zum Beispiel durch ein europäisches Verständnis über Cyberangriffe, vereinheitlichte und gemeinsame Maßnahmen, das Bereitstellen von Möglichkeiten voneinander zu lernen, vergleichende Analysen von Cyberangriffen und Subversion oder durch die stärkere Förderung der EU StratCom.
- Die universelle Gültigkeit von Normen kann erst am Ende eines evolutionären Prozesses stehen, in dem sich der Kreis der Gleichgesinnten sukzessive ausweitet. Gleichgesinnte Staaten können Abkommen zum Verzicht auf Cyberspionage schließen, sie können Cyberdoktrinen austauschen und dem Gegenüber signalisieren, wie man im Falle von Cyberangriffen reagieren würde, so ließen sich auch „rote Linien“ definie-

ren, „rote Telefone“ einrichten oder auch Maßnahmen zur gegenseitigen Unterstützung im Falle von Cyberangriffen abstimmen. Staaten können auch unilateral, als Zeichen der Vertrauensbildung, auf aggressive Formen der Cyberoffensive verzichten.

- Autoritäre Regime, westliche Staaten und private Firmen bedienen sich gleichermaßen der technischen Möglichkeiten zur Sammlung von riesigen Datenmengen, der Spionage, der Beobachtung und Beeinflussung von politischem und sozialem Verhalten und der Förderung regimekritischer Stimmen in gegnerischen Regimen. Der Datenschutz sollte universell Massenüberwachung einschränken und zur informationellen Selbstbestimmung ertüchtigen. Personenbezogene Daten müssen beim Verkehr zwischen Diensten besser geschützt werden. International muss das Völkerrecht auch auf den Cyberraum Anwendung finden.
- Die deutsche Cyber-Außenpolitik sollte die Interessen und Vorstellungen der Bundesrepublik Deutschland in Bezug auf Cyber-Sicherheit in internationalen Organisationen koordinieren und verfolgen. Es gilt, das gemeinsame europäische Handeln bzw. gleichgesinnter Staaten bei Cyberbedrohungen im Angesicht von Bedrohungen und Cyberkampagnen zu stärken. Übergreifende Maßgabe der Auswärtigen Kulturpolitik sollte der Schutz von Menschenrechten, der Erhalt und die Erweiterung von (digitalen) Freiheitsräumen zur transnationalen Vernetzung und für Austausch, das internationale Recht, verantwortungsvolles Staatenhandeln und der Ausbau vertrauensbildender Maßnahmen sein.

Literatur

Abebe, Daniel (2016): Cyberwar, International Politics, and Institutional Design, in: The University of Chicago Law Review 83/1 (Winter), S. 1-22

Adger, W. Neil (2006): Vulnerability. Global Environmental Change 16, S. 268-281

Adkins, Heather; Dmitri Alperovitch; Ryan Borkenhagen; Josh Burek, Michael Chenderlin; Robert Cohen; Chris Collins; Caitlin Conley; Julia Cotrone; Jordan D'Amato; Mari Dugas; Josh Feinblum; John Flynn; Siobhan Gorman; Daniel Griggs; Stuart Holliday; Eben Kaplan; Greg Kesner; Dai Lin; Kent Lucken; Katherine Mansted; Ryan McGeehan; Jude Meche; Nicco Mele; Eric Metzger, Zac Moffatt; Harrison Monsky; Debora Plunkett; Colin Reed; Kim Routh; Suzanne E. Spaulding; Matthew Spector; Irene Solaiman; Jeff Stambolsky; Ales Stamos; Phil Venables; Frank White; Sally White; Rob Witoff (2018): The Cybersecurity Campaign Playbook. Harvard Kennedy School. Belfer Center for Science and International Affairs, May 2018, https://www.belfercenter.org/sites/default/files/files/publication/Campaign-Playbook_0.pdf [23.03.2019]

Anderson, Collin, und Karim Sadjadpour (2018): Iran's Cyber Threat. Espionage, Sabotage, And Revenge, Hrsg. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf [23.03.2019]

Anderson, Collin, und Karim Sadjadpour (2018): Iran's Cyber Threat. Espionage, Sabotage, And Revenge, Hrsg. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf [23.03.2019]

Arquilla, John; David Ronfeldt (1997): Cyberwar is Coming!, in: dies. Athena's Camp. Preparing for Conflict in the Information Age, RAND Corporation, S. 23-60, https://www.rand.org/pubs/monograph_reports/MR880.html [23.03.2019]

Barnes, Julian E. (2018): Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says, in: New York Times 21.12.2018

Bastos, Marco; Dan Mercea (2017): The Brexit Botnet and User-Generated Hyperpartisan News. Social Science Computer Review 20, S. 1-18

Beuth, Patrick, Kai Biermann, Martin Klingst, und Holger Stark (2017): Merkel und der schicke Bär. In Zeit.de 10.05.17. https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/komplettansicht [23.03.2019]

Bing, Christoper, und Joel Schectman (2019): Inside the UAE's Secret Hacking Team of American Mercenaries. In: Reuters 30.01.2019, https://www.reuters.com/investigates/special-report/usa-spying-raven [23.03.2019]

Boemcken, Marc von (2013): Between Security Markets and Protection Rackets: Formations of Political Order: Political Order in Compulsory and Commercial Security Formations, Leverkusen

Brattberg, Erik; Tim Maurer (2018): Russian Election Interference. Europe's Counter to Fake News and Cyber Attacks. Carnegie Endowment for International Peace. Washington: Carnegie Endowment for International Peace, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf [23.03.2019]

Buchanan, Ben (2017): The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations, Oxford

Bundesministerium der Verteidigung (2016): Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundesrepublik, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf [23.03.2019]

Cardenal, Juan Pablo; Jacek Kucharcyk; Grigorij Mesežnikov; Gabriela Pleschová. (2017): Sharp Power. Rising Authoritarian Influence. National Endowment for Democracy, 05.12.17, https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-InfluenceFull-Report.pdf [23.03.2019]

Carpenter, Steve; Brian Walker; J. Marty Anderies; Nick Abel (2001): From Metaphor to Measurement: Resilience of What to What?, in: Ecosystems 4, S. 765-781

Cederberg, Gabriel (2018): Catching Swedish Pish. How Sweden is Protecting its 2018 Elections, Harvard Kennedy School, Belfer Center for Science and International Affairs, August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20-Phish%20%20final2.pdf [23.03.2019]

Chen, Adrian (2015): The Agency, in: The New York Times 02.06.2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html [23.03.2019]

Clarke, Richard A.; Robert K. Knake (2010): The Next threat to National Security and What to Do About It, New York

Clayton, Mark (2014): Ukraine election narrowly avoided 'wanton destruction' from hackers, in: The Cristian Science Monitor 17.07.14, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers [23.03.2019]

Cohen, Howard (2018): Tech Tock...Time is Running Out to Find Solutions to Mis- and Disinformation and Privacy Problems. Harvard Kennedy School, Belfer Center for Science and International Affairs, Mai 2018, https://www.belfercenter.org/sites/default/files/files/publication/PAE%20Cohen%20-%20web.pdf [23.03.2019]

Conley, Heather A. (2018): Successfully Countering Russian Electoral Interference. Center for Strategic & International Studies, June 2018; https://www.csis.org/analysis/successfully-countering-russian-electoral-interference [23.03.2019]

Craig, Anthony, und Brandon Valeriano. 2016. Conceptualisung Cyber Arms Races. 2016 8th International Conference on Cyber Conflict: Cyber Power, Tallinn: NATO CCD COE Publications

Dahlmann, Anja; Marcel Dickow (2019): Präventive Regulierung autonomer Waffensysteme. Handlungsbedarf für Deutschland auf verschiedenen Ebenen. Berlin, SWP-Studie 2019/S 01, Januar 2019

David E. Sanger / Nicole Perlroth. 2019. U.S. Escalates Online Attacks on Russia's Power Grid, in: The New York Times 15.06.19, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage [23.03.2019]

Deibert, Ron (2015): Cyberspace under Siege, in: Journal of Democracy 26, S. 64-78

Federation of American Scientists (o.A.): Presidential Policy Directive / PPD-20, https://fas.org/irp/offdocs//ppd-20.pdf [23.03.2019]

Fireeye (2018): Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East 21.08.18, https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html [23.03.2019]

Flümann, Gereon (2015): Streitbare Demokratie in Deutschland und den Vereinigten Staaten. Der Staatliche Umgang mit nicht gewalttätigem politischem Extremismus im Vergleich, Wiesbaden

Freedman, Lawrence (2013): Strategy. A History, Oxford

Gambino, Lauren (2017): Facebook says up to 10m people saw ads bought by Russian agency, in: The Guardian 03.10.17, https://www.theguardian.com/technology/2017/oct/02/facebook-says-up-to10m-people-saw-ads-bought-by-russian-agency [23.03.2019]

Gartzke, Eric; Jon R. Lindsay (2015): Weaving Tangled Webs: Offense, Defense, and Deception in cyberspace, in: Security Studies 24, S. 316-348

Gartzke, Erik (2013): The Myth of Cyberwar. Bringing War in Cyberspace Back to Earth, in: International Security 38, S. 41-73

Georg Mascolo / Ronen Steinke / Hakan Tanriverdi. (2018): Die Geschichte eines Cyber-Angriffs, in: Süddeutsche Zeitung 22.03.18, https://www.sueddeutsche.de/digital/attacke-auf-auswaertiges-amt-die-geschichte-eines-cyber-angriffs-1.3917502 [23.03.2019]

Georg Mascolo / Ronen Steinke / Hakan Tanriverdi. (2018): Die Geschichte eines Cyber-Angriffs, in: Süddeutsche Zeitung 22.03.18, https://www.sueddeutsche.de/digital/attacke-auf-auswaertiges-amt-die-geschichte-eines-cyber-angriffs-1.3917502 [23.03.2019]

Gorchinskaya, Katya; Olga Rudenko; William Schreiber (2014): Authorities: Hackers foiled in bid to rig Ukraine presidential election results, in: KyivPost 25.05.14, https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukrainepresidential-election-results-349288.html [23.03.2019]

Gorodnichenko, Yuriy; Tho Pham; Oleksandr Talavera (2018): Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USelection, draft 02.09.18, https://eml.berkeley.edu/~ygorodni/Brexit_Election.pdf [23.03.2019]

Grigsby, Alex (2018): Unpacking the Competing Russian and U.S. Cyberspace Resolutions at the United Nations, in: Council on Foreign Relations 29.10.2018, https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations [23.03.2019]

Grundgesetz für die Bundesrepublik Deutschland (2010): Landeszentrale für Politische Bildung Rheinland-Pfalz, Mainz

Hagmann, Jonas (2012): Factsheet Risiko, Verwundbarkeit, Resilienz: Neue Gefahrenkonzepte in der internationalen Sicherheitsanalyse (ed. Risk and Resilience Research Group Center for Security Studies ETH Zürich), März 2012, https://www.files.ethz.ch/isn/164454/Factsheet-RisikoVerwundbarkeit-Resilienz.pdf [23.03.2019]

Hansel, Mischa (2013): Internationale Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung, Wiesbaden

Harris, Mike; Josh Feldberg (2018): 89up releases report on Russian influence in the EU referendum, http://89up.org/russia-report [23.03.2019]

Harvard Kennedy School. Belfer Center for Science and International Affairs Adkins (2018): The Cybersecurity Campaign Playbook, Boston, May, https://www.belfercenter.org/CyberPlaybook [23.03.2019]

Herpig, Sven (2016): Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cyber Security for the State. Hull: University of Hull

Herpig, Sven (2018): Governmental Vulnerability. Assessment and Management. Weighing Temporary Retention versus Immediate Disclosure of 0-day Vulnerabilities. A Proposal Supported by the Transatlantic Cyber Forum. Stiftung Neue Verantwortung, Berlin

Herpig, Sven; Julia Schütze; Jonathan Jones (2018): Der Schutz von Wahlen in vernetzten Gesellschaften. Wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt (hrsg. Stiftung Neue Verantwortung), Oktober 2018, https://www.stiftung-nv.de/sites/default/files/der_schutz_von_wahlen_in_vernetzten_gesellschaften.pdf [23.03.2019]

Hughes, Rex (2010): A Treaty for Cyberspace, in: International Affairs, 86/2 (March), S. 523-541

Hulcoop, Adam; John Scott-Railton; Peter Tanchak; Matt Brooks; Ron Deibert (2017): Tainted Leaks. Disinformation and Phishing With a Russian Nexus, in: citizenlab.ca 25.05.17, https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/#part1 [23.03.2019]

Kahneman, Daniel (2012): Schnelles Denken, Langsames Denken, München 2012

Kello, Lucas (2013): The Meaning of the Cyber Revolution, in: International Security 38, S. 7-40

Kello, Lucas (2018): The Virtual Weapon and International Order, New Haven

Koval, Nikolay (2015): Revolution Hacking, in: Kenneth Geers (ed.): Cyber War in Perspective: Russian Aggression against Ukraine, S. 55-58

Lindsay, Jon R. (2013): Stuxnet and the Limits of Cyber Warfare, in: Security Studies 22, S. 365-404

Lindsay, Jon R., Tai Ming Cheung, und Derek S. Reveron (2015): China and Cybersecurity. Espionage, Strategy and Politics in the Digital Domain. Oxford: Oxford University Press

Lindsay, Jon R.; Erik Gartzke (2019): Cross-Domain Deterrence. Strategy in an Era of Complexity, Oxford

Lobo, Sascha (2017): Plädoyer für einen digitalen Marshallplan Es ist Zeit für das ganz große Datenpaket (27.09.2017), https://www.spiegel.de/netzwelt/netzpolitik/deutschland-braucht-einen-digitalen-marshallplan-sofort-kolumne-a-1170138.html [23.03.2019]

Löwenstein, Karl (1937a): Militant Democracy and Fundamental Rights I, in: The American Political Science Review 31: S. 417-432

Löwenstein, Karl (1937b): Militant Democracy and Fundamental Rights, II, in: The American Political Science Review 31: S. 638-658

Malkki, Leena; Teemu Sinkkonen (2016): Political Resilience to Terrorism in Europe: Introduction to the Special Issue, in: Studies in Conflict & Terrorism 39: S. 281-291

Mannheim, Karl (1943 / 1997): Diagnosis of our Time. Collected Works of Karl Mannheim, vol. III, London

Maurer, Tim (2018): Cyber Mercenaries. The State, Hackers, and Power, Cambridge

McKune, Sarah (2015): An Analysis of the International Code of Conduct for Information Security, Toronto: Munk School, September 28, 2015; https://citizenlab.ca/2015/09/international-code-of-conduct/ [23.03.2019]

Meister, Stefan (ed.) (2018): Understanding Russian Communication Strategy. Case Studies of Serbia and Estonia, Stuttgart: ifa, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-59979-0 [23.03.2019]

Nakashima, Ellen (2019): U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, in: The Washington Post 27.02.19. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.bd1fed0238ba [23.03.2019]

National Cyber Security Centre (2018): Reckless campaign of cyber attacks by Russian military intelligence service exposed 04.10.18. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks- russian-military-intelligence-service-exposed [12.10.2018]

Newman, Lily H (2017): Feds Explain Their Software Bug Stash – But Don't Erase Concerns. In Wired.com 15.11.17. https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/ [03.06.2019]

Office of the Directorate National Intelligence (2017): Intelligence Community Assessment. Assessing Russian Activities and Intentions in Recent US Elections, https://www.dni.gov/files/documents/ICA_2017_01.pdf [23.03.2019]

Popescu, Nico; Stanislav Secrieru (2018): Hacks, Leaks and Disruption. Russian Cyber Strategies. The European Union Institute for Security Studies (EUISS), Chaillot Paper 148, Paris

Ranger, Steve (2018): Why Microsoft is fighting to stop a cyber world war. The tech industry is becoming more worried about a cyberwar arms race. But are the right people listening?, Dec. 12, 2018, https://www.zdnet.com/article/why-microsoft-is-fighting-to-stop-a-cyber-world-war/ [23.03.2019]

Rid, Thomas (2012): Cyber War Will Not Take Place, in: Journal of Strategic Studies 35: S. 5-32

Rid, Thomas (2016): All Signs Point to Russia Being Behind the DNC Hack; in: Motherboard 25.06.16, https://motherboard.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack [23.03.2019]

Rid, Thomas (2016): Rise of the Machines. A Cybernetic History. New York: Norton

Rid, Thomas (2017): Cyber War Will Not Take Place. Oxford: Oxford University Press

Rid, Thomas; Ben Buchanan (2015): Attributing Cyber Attacks, in: Journal of Strategic Studies 38, S. 4-37

Rid, Thomas; Ben Buchanan (2018): Hacking Democacy, in: SAIS Review of International Affairs 38, S. 3-16

Ruhmann, Ingo (2012): Cyber-Krieg oder Cyber-Sicherheit?, in: Wissenschaft & Frieden 4, S. 28–31

Schulze, Matthias, und Sven Herpig (2018): Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them. In: Council on Foreign Relations 03.12.18. https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them?utm_medium=social_share&utm_source=tw [22.03.2019]

Schmitt, Michael N. (2013): Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge

Singer, Peter W.; Emerson T. Brooking (2018): Like War: The Weaponization of Social Media, Boston.

Spahn, Susanne (2018): Russische Medien: Eine Waffe im Informationskrieg. Zentrum liberale Moderne Analyse, 15.11.2018, https://libmod.de/susanne-spahn-ueber-russiche-medien-in-deutschland/ [23.03.2019]

The White House (2017): Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017, Unclassified. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [21.05.2019]

United States District Court for the District of Columbia (2018a): Indictment Case 1:18-cr-00215-ABJ 13.07.18, https://www.justice.gov/file/1080281/download [12.10.2018]

United States District Court for the District of Columbia (2018b): Indictment Case 1:18-cr-00032-DLF 16.02.18, https://www.justice.gov/file/1035477/download [12.10.2018]

United States District Court for The Eastern District of Virginia (2018): AO 91 (Rev 11/11) Criminal Complaint. Case No. 1:18-MJ-464, https://www.justice.gov/opa/press-release/file/1102316/download [31.07.2019]

Valeriano, Brandon; Ryan C. Maness (2015): Cyber War versus Cyber Realities, Oxford
Watts, Clint (2018): Messing with the Enemy. Surviving in a Social Media World of Hackers, Terrorists, Russians and Fake News, New York

Yeli, Hao (2017): A Three-perspective Theory of Cyber Sovereignty, in: PRISM 7/ 2, S. 108-115, https://cco.ndu.edu/PRISM-7-2/Article/1401954/a-three-perspective-theory-of-cyber-sovereignty/ [23.03.2019]

Zetter, Kim (2016): Inside the Cunning, unprecedented Hack of Ukraine's Power Grid. In wired.com 03.03.16, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [15.03.2018]

Über die Autoren

Prof. Dr. Andreas Heinemann-Grüder forscht am Bonn International Center for Conversion und lehrt Politikwissenschaft an der Universität Bonn. Seine Forschungsschwerpunkte sind die postsowjetische Politik, vergleichender Föderalismus, zivil-militärische Beziehungen und irreguläre bewaffnete Gruppen.

Johannes Wiggen studierte Politikwissenschaften und BWL an der Albert-Ludwigs-Universität in Freiburg, der Rheinischen-Friedrich-Wilhelms-Universität in Bonn und der University of Dundee. Während seines Studiums beschäftigte er sich mit den Auswirkungen und Folgen des globalen Wandels auf die EU, deutscher sowie europäischer Außen- und Sicherheitspolitik, Cybersicherheit und Desinformationen.

Die Studie ist im Rahmen des ifa-Forschungsprogramms „Kultur und Außenpolitik“ entstanden und erscheint in der ifa-Edition Kultur und Außenpolitik. Das Forschungsprogramm wird aus Mitteln des Auswärtigen Amts finanziert.

Herausgeber: ifa (Institut für Auslandsbeziehungen e. V.),
Charlottenplatz 17, 70173 Stuttgart,
info@ifa.de, www.ifa.de

Autor: Prof. Dr. Andreas Heinemann-Grüder, Johannes Wiggen M.A.

Redaktion/Lektorat:
ifa-Forschungsprogramm „Kultur und Außenpolitik“

Bildnachweis: Jon Moore / Unsplash

Design: Eberhard Wolf, München

ISBN: 978-3-948205-14-0

DOI: https://doi.org/10.17901/AKBP1.01.2020

Weitere Publikationen der ifa-Edition Kultur und Außenpolitik

Bogula, Werner: Digitale Plattformen für internationale Kulturbeziehungen: Sichere Kommunikation und Kooperation im Netz, Stuttgart: ifa 2019 (ifa-Edition Kultur und Außenpolitik)

de Vries, Gijs: Cultural Freedom in European Foreign Policy Stuttgart: ifa, 2019 (ifa Edition Culture and Foreign Policy)

Higgott, Richard and Virginia Proud: Populist-Nationalism and Foreign Policy. Cultural Diplomacy, International Interaction and Resilience, Stuttgart: ifa, 2017 (ifa Edition Culture and Foreign Policy)

Meister, Stefan (ed.): Understanding Russian Communication Strategy. Case Studies of Serbia and Estonia, Stuttgart: ifa, 2018 (ifa Edition Culture and Foreign Policy)

Weitere Publikationen finden Sie unter: *publikationen.ifa.de*

Subversion im Cyberraum

Sicherheit, Freiheit und Resilienz gegen Angriffe im Netz

„Auch Demokratien wollen im ‚Ausnahmezustand' souverän über kritische Informationsflüsse bestimmen können – und worin dieser ‚Ausnahmezustand' gesehen wird, hängt in hohem Maße von der wahrgenommenen Bedrohung der normativen, moralischen oder politisch-argumentativen Lufthoheit ab."

Die technischen Möglichkeiten der Cyberwelt haben gänzlich neue Potenziale zur Beeinflussung von politischen Präferenzen in anderen Staaten eröffnet. Die Meinungsbildung in offenen Gesellschaften wird zunehmend durch subversive Maßnahmen autoritärer Regime im Internet beeinflusst, wodurch der öffentliche Raum Internet stark eingeschränkt wird. In dieser Studie wird untersucht, wie die Resilienz von offenen Gesellschaften gegen Subversion aus dem Cyberraum gestärkt werden kann, ohne dabei die eigenen Grundsätze preiszugeben. Zunächst wird ein Überblick zu den Diskursen über Cyberbedrohungen gegeben, um sich dann auf die Frage nach der gesellschaftlichen Resilienz zu konzentrieren.

ifa bicc