Cyberangriffe und Trollarmeen

Vom Computerwurm zur Gefahr für die Demokratie

Maximilian L. Knoll

Die Gefahren für die Demokratie sind längst nicht mehr nur analoger Natur. Auch Herausforderungen im digitalen Raum bedrohen nunmehr die Funktionsfähigkeit der demokratischen Ordnung und gelten aufgrund rechtlicher Grauzonen sowie weitgehend ungeklärter Zuständigkeitsfragen als äußerst schwer einzudämmen. An vielen Stellen ist der Staat nicht adäquat gewappnet, um diesen Gefahren entgegenzutreten. Nur ein kluger Spagat zwischen entschlossenem Handeln und Anpassungsfähigkeit kann langfristig zum Erfolg führen.

Als Robert M. Morris im Jahre 1988 den ersten medienwirksamen Computerwurm in seiner Hochschule entwickelt und anschließend in Verkehr gebracht hat, dürfte ihm das, was ab den späten Nullerjahren zunehmend die Regel werden sollte, als Begleiterscheinung futuristischer Dystopien vorgekommen sein. Nicht nur, dass verschiedene Mittel des Cyber- und Informationsraums in feindlicher Willensrichtung einmal eingesetzt würden, um die Präsidentschaftswahlen der rüstigen Demokratien USA und Frankreich zu beeinflussen oder Gaspipelines und Zentrifugen von Atomreaktoren (ohne physische Einwirkung) physisch zu beschädigen. Während Morris immerhin eine Bewährungsstrafe verbüßte, ist es zunehmend schwerer zu ermitteln, wer sich hinter infantil und euphemistisch anmutenden Trollarmeen beziehungsweise Spionage und Erpressungen mit den Namen *CozyBear*, *Sandworm* oder *WannaCry* verbirgt. Die im Verhältnis zur eher unsichtbaren Anbahnung bisweilen zerstörerische, jedenfalls aber kostspielige Reichweite dient dabei häufig als Anlass, sämtliche Katastrophenszenarien aus der analogen in die digitale Welt zu übertragen, indem das Wort „cyber" mit Attributen wie 9/11, Pearl Harbor oder Tschernobyl angereichert wird. Erfahrungsgemäß sind staatliche Einrichtungen hierzulande etwas nüchterner mit apokalyptischen Konnotationen und differenzierter hinsichtlich des Wirkungsgrades.

Ohne Zweifel weisen Angriffe aus dem Cyber- und Informationsraum gesellschaftliche und wirtschaftliche Implikationen auf, sei es in Form von „Nadelstichen", indem verschiedene private oder staatliche Dienste (vorübergehend) nicht in Anspruch genommen werden können, sei es, indem Systeme verschlüsselt werden und deren Weiterverwendung von Lösegeldzahlungen abhängig gemacht wird. Der russische Angriffskrieg auf die Ukraine und ihre Gegenwehr finden auch im Cyber- und Informationsraum statt. Dies mag in Gestalt von kriegsüblicher Propaganda, der Inszenierung eigener Truppen, Geländegewinnen und -verlusten wenig überraschen. Eindrücklich ist vielmehr, wie im Zuge dieses Konflikts nicht nur die Dezentralität derer augenfällig wird, die sich auf den digitalen Austragungsorten betätigen und dazu anlassbezogen zusammenfinden, sondern auch deren Wirkmächtigkeit im Verhältnis zu einem Land wie Russland, das bislang auf dem Gebiet der hybriden (im Sinne des Zusammenwirkens analoger und digitaler) Kriegsführung als besonders versiert galt.

Ist die Funktionsfähigkeit des demokratischen Staates gefährdet?

Ohne der vorgenannten Hyperbel das Wort reden zu wollen, steht angesichts der potenziell weitreichenden Auswirkungen durch Einflussnahme aus dem Cyber- und Informationsraum die Frage im Raum: Kann hiervon auch die Demokratie – als einer der Grundpfeiler unserer staatlichen Organisation – gefährdet sein? Der Abstraktionsgrad könnte kaum höher sein und die Übersetzungsleistung „Herrschaft des Volkes" hilft nur bedingt: Ist die Herrschaft mit der Abgabe der Stimme ausgeübt, oder gehört mehr dazu? Selbst wenn die Abgabe der Stimme ohne Komplikationen abläuft und schließlich auch Teil des Gesamtergebnisses wird, das heißt Zähl- und Erfolgswert einander entsprechen: Welche Rolle spielt das Vertrauen in den individuellen (Wahl-)Prozess aber auch in die Funktionsfähigkeit des Staates als Grundlage für Akzeptanz – und kann es konterkariert werden? Ist der Weg bis hierher gebahnt: Wie und durch wen ist Abhilfe zu schaffen?

Stellt man sich einzelne Elemente von Demokratie als konzentrische Kreise vor, dann befinden sich in der Mitte die eigentliche Wahl bzw. Abstimmung, die Wahlrechtsgrundsätze, die politischen Parteien (als Transmissionsriemen partizipativer Politik) sowie die Mehrheitsentscheidung und der Minderheitenschutz. Während das Prinzip des demokratisch organisierten Staates durch die sogenannte Ewigkeitsklausel grundgesetzlich abgesichert ist, müssen Wahlen nicht nur turnusmäßig stattfinden, sondern auch von einer Mehrheit als ordnungsgemäß durchgeführt anerkannt werden. Das Rezept für Erstgenanntes sind allen voran die Wahlrechtsgrundsätze (insbesondere die Zähl- und Erfolgswertgleichheit der abgegebenen Stimmen), das Rezept für Letztgenanntes ist Akzeptanz, die wiederum Vertrauen voraussetzt und ungleich schwerer zu gewährleisten ist. Damit stellt das Vertrauen, um im Bild zu bleiben, den äußeren Kreis dar, der nicht hinweggedacht werden kann, ohne dass eine jede Wahl ihres Zwecks entledigt und zu einem rein bürokratischen Ereignis degeneriert. Dass es sich hierbei weniger um einen akademischen Diskurs als vielmehr die praktische Realität handelt, lässt sich spätestens seit der Präsidentschaftswahl 2020 in den USA beobachten. Obwohl 64 von 65 Versuchen, Wahlergebnisse auf unterschiedlichen Ebenen gerichtlich anzufechten, scheiterten, glauben bis zu zwei Drittel der US-Republikanerinnen und -Republikaner, dass die Wahl regelwidrig ablief und dies kausal für die Niederlage ihres Kandidaten war.[90]

Mittelbare und unmittelbare Einflussnahme

Wie kann sich nun der Einsatz des Cyber- und Informationsraums auf das engere und weitere Beziehungsgeflecht eines demokratischen Prozesses auswirken? Unabdingbar ist die abstrakte Definition eines Cyberangriffs: Im Kern ist allen Ansätzen gemein, dass unter Zuhilfenahme informationstechnischer Systeme auf rechtlich geschützte Güter eingewirkt wird. Informationstechnische Systeme wiederum lassen sich darauf eingrenzen, dass bei ihnen eine Form von Datenverarbeitung stattfindet bei Verwendung von Binärcodes (bestehend aus 0 und 1).

Ein Versuch der Synthese anhand der dargestellten Elemente ergibt: Die Gefahr, eine Wahl in ihrer postulierten allgemeinen, unmittelbaren, freien, gleichen und geheimen Weise zu konterkarieren, ist formal insoweit beherrschbar, wie sie sich von informationstechnischen Systemen entkoppeln lässt. Sobald jedoch eine Form von Datenübertragung etwa auf einen Server oder in eine Cloud stattfindet, womöglich noch über das Internet, wäre auch eine Einbruchsstelle – jedenfalls in der Theorie – gegeben, die in Verbindung mit dem „Faktor Mensch" eine erfolgreiche Einflussnahme ermöglichen kann. Vor einem Großteil der gängigen Cyberangriffe ließe sich nämlich ungeachtet der lückenhaften Systemarchitekturen nahezu sicher schützen, wenn Menschen insbesondere mit dem Öffnen von E-Mail-Anhängen sorgsamer umgingen. Gerade weil es menschlicher Mitwirkung bedarf, ist der Schutz häufig eine Frage von individueller Sorgsamkeit. Die erfolgreiche digitale Beeinflussung einer Kommunal-, Landtags- oder Bundestagswahl erscheint mit Blick auf deren gegenwärtig analogen Ablauf eher unwahrscheinlich – ein zunächst einmal beruhigendes Zwischenergebnis.

Kommen wir – entlang der oben genannten Kreise – zum Vertrauen als akzeptanzschaffende Basis für einen demokratischen Willensbildungsprozess. Um zunächst einmal beim Wahlgang zu bleiben: Wie lässt sich das Vertrauen auf Zähl- und Erfolgswertgleichheit als dem Kern ordnungsgemäßer Durchführung von Wahlen konterkarieren? Hilfreich ist die Überlegung, wie typischerweise von Wahlergebnissen Kenntnis erlangt wird. Überwiegend dürfte dies über öffentlich-rechtliche und private Medienanstalten erfolgen. Man stelle sich vor, die Hochrechnungen einer Bundestagswahl müssten am Wahlabend wiederholt jenseits der typischen Schwankungen korrigiert werden, weil zum Beispiel auf das Ergebnis der Datenübermittlung eingewirkt worden ist. Oder aber der behördliche Zugriff auf Systeme der Stadt- oder Kreisverwaltungen wird im Rahmen von sogenannten Ransomware-Angriffen gesperrt: So geschehen im Juli 2021, als die Kreisverwaltung Anhalt-Bitterfeld mit knapp 900 Mitarbeiterinnen und Mitarbeitern über Nacht quasi handlungsunfähig wurde.[91]

Gleichsam lässt sich bereits im Vorfeld durch geschicktes Streuen von Falschinformationen das Ergebnis einer Wahl in Zweifel ziehen. Ansatzpunkt könnten etwa die Stimmen der Briefwählerinnen und Briefwähler sein, indem entweder vorgetäuscht wird, diese würden aus welchen Gründen auch immer in das Gesamtergebnis nicht einfließen, oder sie seien bereits ausgezählt worden, verbunden mit erfundenen „Vorab"-Hochrechnungen; beides angereichert durch wirkmächtige Bilder und Videos in sozialen Netzwerken. Die Algorithmen der einschlägigen Netzwerke dienen hierbei als wirksames Vehikel. Die auf Maximierung der Verweildauer der Nutzerinnen und Nutzer angelegten Algorithmen reagieren besonders auf reißerische Darstellungen. Daraus erwachsende „Trends" sorgen dafür, dass die Botschaften einer immer breiteren Öffentlichkeit bekannt werden. Eine Gegendarstellung durch die öffentlich-rechtlichen Sendeanstalten könnte denklogisch nur gegenüber denjenigen verfangen, die ihnen gegenüber aufgeschlossen sind. Definitiv sind solche Ereignisse in der Lage, Vertrauen zu unterminieren, das sich zumeist schwerer zurückgewinnen als initial stören lässt.

Jenseits der Beeinflussung des Wahlergebnisses ist eine weitere Ebene nicht zu vernachlässigen, die weniger auf den demokratischen Ablauf im engeren Sinne abstellt, als vielmehr auf den Meinungsbildungsprozess im Vorfeld. So kann es unmittelbar Auswirkung auf das Wahlverhalten haben, wenn Wahlkampfteams kompromittiert werden, indem auf interne Kommunikation (wie E-Mails) zugegriffen und diese (entsprechend der eigenen Agenda) veröffentlicht wird. Dass dies nicht aus der Luft gegriffen ist, zeigt ein Blick in das Jahr 2017, als im Zuge des „Macron-Hack" einen Tag vor der Stichwahl im Rahmen der französischen Präsidentschaftswahlen mehr als 20.000 gestohlene E-Mails aus dem Wahlkampfteam einer der Kandidaten veröffentlicht wurden;[92] dies wohlgemerkt zu einem Zeitpunkt, als Wahlwerbung gesetzlich nicht mehr erlaubt war, die Inhalte also unkommentiert im Raum standen.

Abgesehen von den dargestellten Möglichkeiten, mit Cyberangriffen auf staatliche Institutionen und Abläufe einzuwirken, darf ein weiterer Aspekt nicht unberücksichtigt bleiben, der die vorherigen Aspekte einschließt und mittelbar Bezug zum demokratischen Prozess aufweist: die Funktionsfähigkeit des Staates und das Vertrauen hierauf. Besonders wirkmächtig dürfte in diesem Zusammenhang wohl der Angriff auf das Netzwerk des Deutschen Bundestages im Jahr 2015 sein.

Von zentraler Relevanz ist hier aber auch das staatliche Gewaltmonopol. Inhaltlich ist damit gemeint, dass der Staat mit seinen Institutionen im Rahmen der Gesetze befugt und mitunter verpflichtet ist, wesentliche Schutzfunktionen gegenüber den Bürgerinnen und Bürgern selbst wahrzunehmen. Während dies allgemein und nicht speziell für Gefahren aus dem Cyberraum gilt, ist es hier aber besonders herausgefordert.

Der Staat verliert seine „Lufthoheit“

Während Angreiferinnen und Angreifer aus dem Cyberraum stärker werden und sich zunehmend in Sicherheit wiegen, sieht sich der Staat mit institutionellen und organisatorischen Herausforderungen konfrontiert. Ein Blick auf die Nachrichtenlage zeigt, dass Ereignisse wie *Stuxnet*, Angriffe mit flächendeckendem Ausfall der Stromversorgung und sonstige apokalyptisch anmutende Ereignisse im Verhältnis zu dem, was als Cyberkriminalität verstanden wird, bisher – zum Glück – eine untergeordnete Rolle gespielt haben. Cyberkriminelle zielen insbesondere auf Teile der sogenannten öffentlichen Daseinsvorsorge (wie Krankenhäuser) ab sowie in rasant zunehmendem Maße auf privatwirtschaftliche Einrichtungen, mittelständische Firmen und Industriebetriebe.[93] Der Angriff zeigt sich in der Regel dergestalt, dass bei einer *Zero-Day*-Sicherheitslücke[94], die als E-Mail-Anhang oder Link getarnt ist, der Zugang zum jeweiligen Betriebsnetzwerk verschlüsselt wird und die Wiederherstellung des Zugangs von der Zahlung eines Lösegeldes (daher Ransomware-Angriff genannt) in Kryptowährung abhängig gemacht wird. Flankiert wird das Vorgehen in aller Regel mit der Veröffentlichung von Firmengeheimnissen, vertraulichen Daten oder (vorgeblich) kompromittierendem Material über Firmenvertreterinnen und -vertreter, wodurch der monetären Forderung Nachdruck verliehen wird. Nur die wenigsten Betroffenen erhalten nach Zahlung sämtliche Daten zurück. Diese Ereignisse nehmen weltweit rasant zu, zwischen 2019 und 2020 ist allein ein Anstieg von 485 Prozent verzeichnet worden.[95]

In den Fällen der vorgenannten Ransomware-Angriffe wird eine besondere Disparität augenscheinlich. So werden die Angriffe von arbeitsteilig und global organisierten Zusammenschlüssen und Banden unterschiedlicher fachlicher Hintergründe durchgeführt. Dreh- und Angelpunkt sind Plattformen, auf denen sich die Beteiligten ad hoc „projektbezogen“ zusammenfinden. Der Bedarf an terrestrischer Infrastruktur geht gegen Null und beschränkt sich maximal auf einen Funkmast in der weiteren Umgebung; ist dieser vorhanden, ist nur noch Strom für den Betrieb der eigenen Endgeräte nötig. Der Aufenthaltsort und die Jurisdiktion sind dagegen unerheblich. Im Darknet werden die IP-Adressen nicht protokolliert, selbst wenn: Die Dezentralität ermöglicht (auch bei geglückter Rückverfolgung), den eigenen Standort zu verschleiern, sofern dieser nicht ohnehin in anderen Staaten liegt und der Erfolg der Strafverfolgung dadurch erheblich beeinträchtigt ist.

Ein weiterer wesentlicher institutioneller Aspekt ist die Organisation auf staatlicher Ebene. Der Bund ist bis auf wenige Ausnahmen im (vollzugs-)polizeilichen und nachrichtendienstlichen Bereich im Inland nur koordinierend tätig. Dies zeigt eine weitere Schwierigkeit: Während die Auswirkungen unzweifelhaft und sichtbar im Inland sind, ist regelmäßig unklar, wo sich die Urheberinnen oder Urheber befinden. Die Schwierigkeit der Zurechnung eines Cyberangriffs resultiert zum einen aus der institutionalisierten Dezentralität des Cyberraums, zum anderen aus der hieraus entspringenden Möglichkeit der Anonymität und Verschleierung. Das Resultat ist eine in technischer Hinsicht unzureichende, bisweilen unmögliche Rückverfolgbarkeit (*back-tracing*). Dies fordert einen entlang der Trennlinie zwischen „innen“ und „außen“ organisierten Staat heraus. Hieran können auch die Bundeswehr und das dort 2017 aufgestellte Kommando Cyber- und Informationsraum (CIR) nichts ändern, da die Streitkräfte nur entlang des ihnen zugewiesenen gesetzlichen Leitbildes operieren, es aus sich heraus aber nicht fortentwickeln dürfen.

Was gegen Cyberattacken getan wird – und getan werden muss

Nun lässt sich aus dem staatlichen Gewaltmonopol weder ein Anspruch ableiten, der den Staat über den Schutz seiner eigenen Einrichtungen hinaus verpflichtet, vor jedwedem Blackout zu schützen oder sämtliche Gewerbebetriebe schadlos zu halten, noch einseitig eine Prävention zu leisten. Dem hält bereits der analoge Vergleich nicht stand, bei dem die Eigenverantwortlichkeit wesentliches Merkmal und letztlich die Kehrseite allgemeiner Handlungsfreiheit darstellt. Wenn es aber um strukturelle Organisationsleistungen geht, sind diese durch die Betroffenen aber gerade nicht zu bewältigen, sondern typischerweise staatliche Aufgabe.

Zentrale Punkte sind hierbei die Behördenausstattung und -organisation. Ausstattung meint dabei Personal und Material. Beides bedingt einander. Nicht hinreichend qualifiziertes Personal kann keine mündigen Entscheidungen für die materielle Ausstattung treffen, geschweige denn die Organisation anpassen. Die Folge ist bekannt: Abhängigkeit von Beratungsunternehmen und sonstigen Dienstleistern, die den Staat als blauäugigen Kunden schätzen; sinnbildlich in diesem Zusammenhang die sogenannte Corona-Warn-App, die bereits einen hohen dreistelligen Euro-Millionenbetrag verschlungen hat.[96] Beim Personal ist zu erkennen, dass die qualifizierten Köpfe ihren Preis haben. Für entsprechende IT-Spezialistinnen und –Spezialisten oder ganz konkret Hackerinnen und Hacker, um im Thema zu bleiben, werden nicht zuletzt seitens der *GAFAM* (Google, Amazon, Facebook, Apple und Microsoft) regelmäßig Gehälter bezahlt, die weit jenseits behördlicher Besoldung sind. Während der Markt-

preis zunächst einmal hinzunehmen ist, lässt sich die Vergütung wettbewerbsgerecht anpassen. Dazu bedarf es aber der Erkenntnis, dass Kompetenz und Fähigkeit die entscheidenden Kriterien sind, nicht zwingend die jeweilige Ebene in der Hierarchie oder gar die Dauer der Zugehörigkeit zu einer Verwaltungseinheit. Warum darf eine qualifizierte Person nicht mehr kosten als andere auf ihrer hierarchischen Ebene, wenn sonst externer Sachverstand eingekauft werden müsste, bei dem das Verhältnis von Aufwand und Ertrag der zuvor erwähnten Gefahr ausgesetzt ist? Erschwerend kommt hinzu, dass der Wechsel von der Privatwirtschaft in die Verwaltung und zurück in Deutschland grundsätzlich nicht vorgesehen ist. Wie aber soll ein am Puls der Zeit orientierter Schutz aufgebaut und vor allem laufend angepasst werden, wenn die personelle Interaktion mit der (zumal finanzstarken) Fachwirtschaft nicht möglich ist? All dies lässt sich ändern, entscheidend ist, dass der Handlungsbedarf erkannt wird.

Die Problematik der Attribution von Cyberangriffen hat unmittelbaren Einfluss auf die Staatsorganisation: Das beginnt bei den Kompetenzen (Wer ist wofür zuständig?) und endet bei der Organisation der Verwaltungseinheit. Auch hier ist die Wechselbeziehung mit der personellen Ausstattung augenfällig. Da entsprechendes Personal knapp ist, ist es unklug, sämtliche Strukturen für jedes Bundesland und den Bund (das heißt 16 bzw. 17 Mal) vorzuhalten. In zuständigkeitsbezogener Hinsicht ist ferner die Grundannahme für die Kompetenzverteilung zu überdenken: Weil Angriffe regelmäßig nicht nach äußerer oder innerer Urheberschaft differenziert werden können, macht eine Behördenorganisation entlang dieser Trennlinie wenig Sinn. Effektiver wäre es, diesen Bereich ganzheitlich zu verstehen, ihn von sonstigen Sicherheitsaufgaben zu entkoppeln und entlang von Szenarien oder verschiedenen Beeinträchtigungsgraden zu organisieren. Eine solche Modifizierung könnte Landes- und Bundesbehörden, Polizeien und Nachrichtendienste, aber auch die Streitkräfte in den Blick nehmen. Das vorhandene Nationale Cyber-Abwehrzentrum und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich sind jedenfalls kein Ersatz, da sie nur behörden- und institutionenübergreifende Plattformen darstellen, mit denen versucht wird, die Defizite des Status quo abzufedern. Im Grunde ist ihre Existenz Nachweis für den beschriebenen Handlungsbedarf. Im Zentrum müssen dabei Fähigkeiten stehen, nicht Behördennamen. So sind die Streitkräfte mit ihrem Kommando CIR nicht von vornherein am oberen Ende einzuordnen, nur weil sie im kinetischen Bereich die wirkmächtigsten Fähigkeiten besitzen. Im Gegenteil: Um der Debatte des militärischen Inlandseinsatzes zu entgehen, wäre es vielleicht sogar sinnvoll, die Cyberabwehr ganz losgelöst von den Streitkräften zu organisieren. Zu den Fähigkeiten gehört, betroffene IT-Strukturen aufzuklären, zu isolieren, zu reparieren sowie wenn möglich und geboten: zurückzuschlagen.

Im Zentrum müssen Fähigkeiten stehen, nicht Behördennamen.

Im Bereich der Resilienz und Prävention wurde dagegen bereits begonnen, Lasten zu verteilen. So legen die europäischen Rechtsakte zur Cybersicherheit sowie das nationale IT-Sicherheitsgesetz 2.0 Unternehmen, insbesondere solchen mit *kritischer Infrastruktur,* immer strengere Sicherheitsmaßnahmen auf. Der Staat kann den Schutz in der Breite nicht selbst leisten und nimmt die Privatwirtschaft zunehmend in die Pflicht. Beides ist geeignet, die dem Gewaltmonopol innewohnende Aufgabenverteilung zwischen Bürgerschaft und Staat in Richtung eines partnerschaftlichen Miteinanders zu modifizieren. Das kann auch Konsequenzen haben. Sofern der Einzelne mehr in die Pflicht genommen wird, kann dies Begehrlichkeiten wecken. Das „Über-/Unterordnungsverhältnis“ zwischen Staat und Bürgerinnen und Bürgern kann sich verändern. Dies dürfte sich mittelfristig am stärksten dort manifestieren, wo sich der Staat (ausländischer) privater Entitäten behilft, seine eigene IT-Sicherheit zu gewährleisten; neue und historisch eher ungewöhnliche Abhängigkeiten entstehen. Selbst wenn einige der zuvor beschriebenen Strukturmaßnahmen ergriffen werden, wird sich wohl keine vollständige Entkopplung von privater Seite erzielen lassen: Dafür sind der staatliche Nachholbedarf in den erwähnten Bereichen zu erheblich, aber auch die übrigen (sozial)staatlichen Verpflichtungen zu groß, die ebenfalls nicht aus dem Fokus geraten wollen.

Die wesentlichen Assets unseres Staates sind zweierlei. Erstens ist seine im demokratischen Prozess sich fortlaufend erneuernde Ordnungshoheit zu nennen. Diese muss er geschickt nutzen, um seine „Lufthoheit“ gegenüber Einflüssen von Dritten zu wahren. Dass dies organisatorisch im größtmöglichen Rahmen angegangen werden sollte und damit eher europäisch, wenn möglich auch transatlantisch, versteht sich dabei aus der Natur der (entgrenzten) Thematik selbst sowie dem Umstand, dass offene, freiheitliche Demokratien typischerweise ähnliche Verwundbarkeiten aufweisen. Hier sind im Wege eines Europäischen Rechtsakts zur Cybersicherheit sowie der Etablierung eines EU-weit geltenden Rahmens für die Zertifizierung von IT-Sicherheitsprodukten kluge Schritte gemacht worden. In inhaltlicher Hinsicht gehört zur Ordnungshoheit aber auch, zum eigenen Wohl geeignete Instrumente einzusetzen und deren Wirksamkeit fortlaufend zu überprüfen. Die Wirksamkeit ist insbesondere dort abzuklopfen und gegebenenfalls anzupassen, wo (extraterritoriale) Gegnerinnen und Gegner auftreten, die versuchen, offene – weil systemimmanente – Flanken freiheitlicher Demokratien auszunutzen. Konkret heißt das: Wenn der Cyber- und Informationsraum als Machtinstrument genutzt wird, um demokratische Abläufe- und Meinungsbildungsprozesse zu stören, sollte als Mittel der Abschreckung der Einsatz vergleichbarer Mittel nicht ausgeschlossen werden.[97] Dass Staaten hier generell Nachholbedarf aufweisen, lässt sich auch beim Ukraine-Krieg belegen: Wenn sich der ukrainische Vizepräsident mit der Auf-

forderung an die weltweite Hacker-Gemeinschaft wendet, Russlands staatliche Webseiten und digitale Infrastruktur ins Fadenkreuz zu nehmen,[98] ist dies nicht nur ein weiterer Beleg für die Existenz der zuvor angeführten Ad-hoc-Kräfte, sondern auch für deren Wert als kritische, weil unzureichend im Dienste des Staates vorhandene Ressource zur Gefahrenabwehr oder gar Landesverteidigung.

Das zweite wesentliche Asset ist ein Alleinstellungsmerkmal: Nur der Staat kann von sich behaupten, kraft des demokratischen Willensbildungsprozesses dem Gemeinwohl verpflichtet zu sein. Dieser Tatsache kommt ein entscheidender Wert in einer Zeit zu, wo private Kräfte an Macht und Einfluss gewinnen und in der Lage sind, das klassischerweise vom Staat beanspruchte Gewaltmonopol – wie aufgezeigt – partiell herauszufordern. Im Unterschied zum Staat sind private Akteurinnen und Akteure nicht dem Gemeinwesen verpflichtet. Hier liegt der entscheidende Unterschied, der doch geeignet sein sollte, für Legitimität und Akzeptanz zu sorgen.

Autor

Dr. Maximilian L. Knoll war Promotionsstipendiat der Konrad-Adenauer-Stiftung.

90 Gellman, Barton 2021: Trump's next coup already begun, The Atlantic, 06.12.2021, in: https://www.theatlantic.com/magazine/archive/2022/01/january-6-insurrection-trump-coup-2024-election/620843/ [23.02.2022].

91 Locke, Stefan 2021: Hacker legen Verwaltung von Anhalt-Bitterfeld lahm, Frankfurter Allgemeine Zeitung, 13.07.2021, in: https://www.faz.net/aktuell/politik/inland/anhalt-bitterfeld-hacker-legen-verwaltung-lahm-17436039.html [23.02.2022].

92 Bundesamt für Sicherheit in der Informationstechnik 2021: Die Lage der IT-Sicherheit in Deutschland 2021, in: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3 [23.02.2022].

93 Adam, Sally 2021: The State of Ransomware 2021, Sophos, 27.04.2021, in: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/ [23.02.2022].

94 Ausgangspunkt ist die „Rückübersetzung" des Programmcodes. Diese erfolgt über das sogenannte Reverse Engineering. Der Programmcode wird wieder sichtbar gemacht. Im Zuge der Visualisierung des Codes werden nun auch Einbruchstellen offengelegt. Diese Einbruchsstellen heißen „Zero Days", weil sie vor ihrer Entdeckung nicht vorhanden waren, also „Null Tage" existent.

95 Coker, James 2021: Ransomware Attacks Grew by 485% in 2020, Infosecurity Magazine, 06.04.2021, in: https://www.infosecurity-magazine.com/news/ransomware-attacks-grow-2020/ [23.02.2022].

96 Antwort der Bundesregierung vom 14.01.2022 auf eine Kleine Anfrage der Fraktion AfD (auf Bundestagsdrucksache 20/431), in: https://dserver.bundestag.de/btd/20/004/2000431.pdf [24.04.2022].

97 Gordon, Sue/Rosenbach, Eric 2022: America's Cyber-Reckoning, Foreign Affairs, 1/2-2022, in: https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning [23.02.2022].

98 Pearson, James 2022: Ukraine launches „IT army", takes aim at Russian cyberspace, Reuters, 26.02.2022, in: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/ [24.04.2022].