SWP

SWP-Aktuell

NR. 12 FEBRUAR 2021

EU-Strategie zur Cybersicherheit: Desiderat Cyberdiplomatie

Annegret Bendiek/Matthias C. Kettemann

Im Dezember 2020 hat die Europäische Union (EU) ihre neue Strategie zur Cybersicherheit vorgelegt mit dem Ziel, Europas technologische und digitale Souveränität zu stärken. Das Dokument listet Reformvorhaben auf, die die Cybersicherheit enger mit den neuen EU-Regeln zu Daten, Algorithmen, Märkten und Internetdiensten verbinden sollen. Eindeutig zu kurz geraten ist dabei jedoch der Aufbau einer europäischen Cyberdiplomatie, die sowohl der »strategischen Offenheit« als auch dem Schutz des digitalen Binnenmarktes verpflichtet ist. Um dies zu erreichen, sollte die EU-Cyberdiplomatie in ihrer supranationalen, demokratischen und wirtschaftlichen bzw. technologischen Dimension kohärenter ausgestaltet werden. Deutschland kann hierzu einen wichtigen Beitrag leisten, indem es dem Europäischen Auswärtigen Dienst (EAD) die notwendigen rechtlichen, fachlichen und finanziellen Ressourcen zur Verfügung stellt.

Die EU registrierte 2019 rund 450 Angriffe auf kritische Infrastrukturen (KRITIS) der Energie- und Wasserversorgung sowie der Informations- und Kommunikationstechnologien im Gesundheits-, Verkehrs- und Finanzwesen. Die Vulnerabilitäten technologisch interdependenter Gesellschaften sind während der Covid-19-Pandemie besonders deutlich geworden. Im vergangenen Dezember haben Cyberkriminelle die Europäische Arzneimittel-Agentur ins Visier genommen. Um ihr gesellschaftspolitisches Modell bewahren zu können, muss sich die EU in einem sicherheitspolitischen Umfeld behaupten, das geprägt ist von wechselseitigen Bedrohungswahrnehmungen und einem an Dynamik gewinnenden Technologie- und Rüstungswettlauf zwischen Staaten. Der Direktor des Technology and National Security Program am Center for a New American Security, Paul Scharre, hat schon vor einiger Zeit darauf verwiesen, dass der Technologiewettlauf das Sicherheitsdilemma des Nuklearzeitalters zu wiederholen drohe (*Foreign Affairs*, Mai/Juni 2019). Wie reagiert nun die EU strategisch auf die veränderten weltpolitischen Rahmenbedingungen? Welche Rolle kann sie spielen, damit Cyberangriffe zum Beispiel auf Kraftwerke im Vorfeld verhindert werden können? Existieren europäisch abgestimmte Verfahren, um im Bedarfsfall unverzüglich und umfassend handeln zu können?

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

EU-Strategie zur Cybersicherheit

Die EU arbeitet bereits seit 2015 an ihren Reaktionsmöglichkeiten auf Attacken aus dem und Konflikte im Cyber- und Informationsraum (CIR). Einige außen- und sicherheitspolitische Initiativen sind in den letzten Jahren auf den Weg gebracht worden (vgl. SWP-Aktuell 22/2018). Zu nennen sind hier unter anderem der Diplomatische Reaktionsrahmen (Cyber Diplomacy Toolbox) und der Politikrahmen für die Cyberabwehr (Cyber Defence Policy Framework) (beide 2018), der Rechtsakt zur Cybersicherheit und die 5G-Toolbox (beide 2019), die Strategie für die Sicherheitsunion und das Screening von (Digital-)Investitionen (2020). Seit 2020 konzentriert die EU ihre Aktivitäten zusammen mit den Mitgliedstaaten auf den Aufbau operativer Kapazitäten zur Prävention und Abschreckung von sowie Reaktion auf schwerwiegende Cybervorfälle in Europa. Den aktuellen Rahmen setzt die im Dezember 2020 von der EU-Kommission und dem Hohen Vertreter für Außen- und Sicherheitspolitik, Josep Borrell, vorgestellte neue Strategie der EU für Cybersicherheit und Resilienz. Sie ist eng mit anderen Initiativen der Union verknüpft, etwa zur digitalen Zukunft des Binnenmarktes, mit dem Konjunkturprogramm der Kommission und der Strategie für die Sicherheitsunion 2020—2025.

Die neue Cybersicherheitsstrategie beinhaltet Folgendes: Eine »gemeinsame Cyberstelle« wird eingerichtet. Sie hat die Aufgabe, die IT-Fähigkeiten von »Verteidigungskreise[n] im Bereich der Cybersicherheit« und die der Strafverfolgungsbehörden in Kooperation mit »zivile[n] und diplomatische[n] Gemeinschaften« zu stärken. Laut der Strategie wird die EU sich auch auf die Arbeiten der Europäischen Verteidigungsagentur stützen und die Zusammenarbeit im militärischen Bereich fördern, wobei sie auf den neu geschaffenen Europäischen Verteidigungsfonds zurückgreifen kann. Des Weiteren soll die EU einen »›Cybersicherheitsschutzschild‹« erhalten, um Gefahren frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten, bevor Schäden entstehen. Die Kommission will ein EU-weites »Netz von Sicherheitseinsatzzentren« aufbauen. Es soll den für Cybersicherheit zuständigen zivilen und militärischen Behörden von Union und Mitgliedstaaten als Kooperationsplattform dienen und die Koordination bei großen Angriffen verbessern. Zum Schutz kritischer Infrastrukturen sollen geltendes EU-Recht und die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) von 2016 überarbeitet und Künstliche Intelligenz stärker genutzt werden, um Cyberattacken gegen Krankenhäuser, Versorgungseinrichtungen oder Verkehrsnetze zu identifizieren.

Seit 2018 verfügt die EU über die Cyber Diplomacy Toolbox, um schwerwiegende Cyberangriffe abwehren zu können (vgl. SWP-Aktuell 22/2018). Sie hat damit ein eigenes Sanktionsregime gegen IT-Angriffe konzipiert, das im Juli 2020 im Zuge der technischen und rechtlichen Aufarbeitung der Hackerangriffe auf den Bundestag 2015 zum Einsatz kam. Zur Umsetzung der Cybersicherheitsstrategie sollen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) Vorschläge für eine Erweiterung des »EU-Instrumentariums für die Cyberdiplomatie« unterbreitet werden, damit Attacken auf die kritische Infrastruktur, Versorgungsketten und die demokratischen Institutionen und Prozesse wirkungsvoll begegnet werden kann.

Zwar verweist die Cybersicherheitsstrategie auf EU-Initiativen wie diejenige zur Bekämpfung hybrider Bedrohungen, auf den Europäischen Aktionsplan für Demokratie und das Notfall- und Krisenmanagement in der EU; die Vertiefung der vertrauens- und sicherheitsbildenden Maßnahmen der EU-Cyberdiplomatie gegenüber Drittstaaten bleibt indes weitgehend unterbelichtet. Die Notwendigkeit solcher Maßnahmen wird festgestellt, jedoch ohne konkrete Beispiele zu nennen oder institutionelle Orte, die sie umsetzen sollen. Damit bringt die Cybersicherheitsstrategie ein vereinseitigtes Verständnis von Sicherheitspolitik zum Ausdruck, das von einem geringen Bewusstsein dafür zeugt, dass technische und technokratische Maßnahmen diplomatisch begleitet werden müssen.

Desiderat Cyberdiplomatie

Die Einseitigkeit der EU-Cybersicherheitsstrategie ist ein Problem, weil internationale Normenbildung ein zentrales Element für Vertrauen und Sicherheit im Cyber- und Informationsraum ist. Der EAD muss genau für diese Aufgabe der Cyberdiplomatie befähigt werden, indem sein Mandat entsprechend ausgerichtet wird. Die derzeitige Strategie vernachlässigt die wichtige Lehre des Nuklearzeitalters, dass Abrüstung und vertrauensbildende Maßnahmen zu allgemein erhöhter Sicherheit führten. Der Politikwissenschaftler Joseph S. Nye argumentiert etwa, entgegen weitläufiger Meinung könne Abschreckung im Cyberspace doch funktionieren. Er sei überzeugt, die bisher sehr begrenzte internationale Normenentwicklung zeige durchaus positive Effekte auf die Sicherheit im CIR. Hierfür sei wesentlich, das Prinzip der Abschreckung nicht auf die klassische territoriale Verteidigung und unmittelbare Vergeltung zu beschränken. Vielmehr würden Kosten-Nutzen-Analysen zu nichtintendierten Folgekosten potentielle Angreifer von Attacken abhalten.

Die Tatsache, dass ein »Cyberwar« bislang noch nicht stattgefunden hat, kann als Indiz für die Wirksamkeit dieser Strategie gewertet werden. Auch können internationale Normenprozesse staatliche Akteure von Maßnahmen gegen kritische Infrastrukturen abbringen. Die Normen für verantwortliches Staatenverhalten im Cyberspace, entwickelt von der Group of Governmental Experts (GGE) der Vereinten Nationen (VN), verbieten Angriffe gegen kritische Infrastrukturen. Die Verhandlungen der VN-Generalversammlung belegen, dass trotz politischer Differenzen an gemeinsamen Normen für rechtmäßiges staatliches Verhalten und an Sorgfaltspflichten im Cyberraum gearbeitet wird. Im Rahmen der Cyber Diplomacy Toolbox ist die Horizontale Ratsarbeitsgruppe zu Cyberfragen (HWP ERCHT) mit diesen Fragen betraut; bisher hat sie jedoch nur eine koordinierende und keine gestaltende Funktion innerhalb der EU-Cyberdiplomatie.

Noch wenig konsentiert sind darüber hinaus Normen zur Reaktion auf Cybermaßnahmen unterhalb völkerrechtlich relevanter Schwellen (Retorsion), Normen für die Zulassung von Hard- und Software, zum Umgang mit Lieferkettenabhängigkeiten und zum Schwachstellenmanagement. Auch das »Non-Paper« von Deutschland und fünf weiteren EU-Mitgliedstaaten vom 19. November 2020 bleibt im Hinblick auf konkrete Maßnahmen unklar. Die Gefahren, die von Proxys, also nichtstaatlichen Akteuren, die im staatlichen Auftrag handeln, ausgehen, schmälern die Effektivität vertrauens- und sicherheitsbildender Maßnahmen. Die Budapest-Konvention des Europarats soll entsprechend überarbeitet werden, um mit einem zweiten Zusatzprotokoll effektiver gegen nichtstaatliche Cyberkriminalität vorgehen zu können. Eine weitere nicht zu unterschätzende Gefahrenquelle ist die hohe Zahl niederschwelliger Angriffe, etwa gegen mittelständische Unternehmen. Geklärt werden muss noch, was als kritischer IT-Sicherheitsvorfall gilt, der gemeldet werden muss, auch Partnerstaaten außerhalb Europas: Wenn der Angreifer ins Netzwerk eindringt und es stört oder schon dann, wenn er die Infrastruktur einer potentiellen KRITIS-Anlage scannt und versucht Schwachstellen zu finden?

Die Cybersicherheitsstrategie erwähnt ferner ein gemeinsames, zwischen Nato und EU abgestimmtes Lagebild im CIR, bleibt aber unspezifisch, was dessen Umsetzung betrifft. Das Potential des in Helsinki ansässigen European Centre of Excellence on Countering Hybrid Threats zum Aufbau der »Legal Resilience« in Bezug auf staatliche Einmischungen wird für die EU—Nato-Zusammenarbeit ebenso wenig ausgeschöpft. Die einen Regierungen sprechen sich für aktive Gegenmaßnahmen nach dem Vorbild der USA aus, die im Cyberspace ihre Vormachtstellung demonstrieren. Andere dagegen plädieren für die Ausarbeitung eines konsentierten Referenzrahmens, der den Staaten Rechenschaftspflichten hinsichtlich ihrer Resilienzmaßnahmen zuweist, um Konflikteskalation im Cyber- und Informationsraum zu verhindern. Beide Ansätze ver-

sucht die EU-Strategie besser als bisher zu integrieren. Um diese Ambition umzusetzen, muss der EAD künftig personell, finanziell und rechtlich stärker mandatiert werden.

Digitale Souveränität und Resilienz sind nur als gesamteuropäische und -gesellschaftliche Aufgabe in enger Abstimmung auf EU-Ebene und mit demokratischen Partnern zu erreichen, zudem muss wirtschaftspolitische und technologische Kompetenz ausdrücklich einbezogen werden. Das bedeutet: Die EU-Cyberdiplomatie muss hierfür die Rahmenbedingungen setzen, da der CIR nicht an Zuständigkeiten und Grenzen der einzelnen Länder gebunden ist. Öffentliche Institutionen, Wirtschaft, Wissenschaft und Zivilgesellschaft müssen viel intensiver als bislang europäisch Hand in Hand arbeiten. Die Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und eines Netzes nationaler Koordinierungszentren sind ein erster richtiger Schritt. Die Cyberdiplomatie kann EU-intern wie nach außen die supranationalen, demokratischen, wirtschaftlichen und technologischen Voraussetzungen schaffen, um die dafür notwendige Infrastruktur, das Know-how und die nötige Spitzentechnologie vorhalten zu können.

Die supranationale Dimension

Sektoral konzipierte Politiksilos, in denen die digitale Dimension von Außen-, Verteidigungs- und Innenpolitik nebeneinander gedacht wird, eignen sich bekanntermaßen wenig für die Cybersicherheit. Sinnvoll erscheint hingegen ein von der EU-Kommission unterstütztes Ineinandergreifen von Regulierungen des Binnenmarktes, Bekämpfung der Cyberkriminalität, GASP bzw. Gemeinsamer Sicherheits- und Verteidigungspolitik (GSVP) sowie Initiativen der Ständigen Strukturierten Zusammenarbeit (PESCO). Ein jährlicher Umsetzungsbericht, angelehnt an die Fortschrittsberichte zur Umsetzung der Sicherheitsunion, wäre förderlich und sollte bisher vernachlässigte Aspekte, wie die technische Aufklärung und den Informationsaustausch, stärker berücksichtigen.

Insbesondere sollten systematisch erfasst werden: die Vorbereitung und der Einsatz von Cyberangriffen; das Manipulieren und Sabotieren von Unternehmen, Finanz- und Industriemärkten; die steigende Anfälligkeit kritischer Infrastrukturen; die wachsende Bedrohung der Zuverlässigkeit traditioneller Verteidigungssysteme durch militärische Hacker. Der neue Strategische Kompass zur Bedrohungslage soll zwar gemeinsame EU-Lagebilder ermöglichen; hierzu müssen aber Sicherheitsbehörden in der inneren und äußeren Cybersicherheit bereit sein, ihre Erkenntnisse im benötigten Umfang im EAD zu bündeln. Die Lagebild-Erstellung soll zumindest in einem ersten Schritt durch eine »horizon scanning«-Fazilität untermauert werden. Künstliche Intelligenz soll dabei helfen, eine Krisenfrüherkennung zu etablieren.

Daran anknüpfen sollte die Entwicklung eines Attributionsverfahrens im GASP-Verfahren. Bis dato gibt es keine gemeinsamen Standards, um den Verursacher eines Cyberangriffs eindeutig zu identifizieren. In den »Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities« (DIG) heißt es, dass die Mitgliedstaaten unterschiedliche Methoden und Verfahren für die Zuordnung böswilliger Cyberaktivitäten sowie unterschiedliche Definitionen und Kriterien anwenden können, »um einen gewissen Grad an Sicherheit für die Zuordnung einer böswilligen Cyberaktivität zu erreichen«. Die Methoden, Verfahren, Definitionen und Kriterien der Mitgliedstaaten sollen jedoch nicht harmonisiert werden, da die Attribution ein hoheitlicher Akt bleiben soll. Der EAD mit seinem Intelligence Analysis Centre (EU INTCEN) müsste neue personelle und fachliche Kompetenzen erhalten, soll er öffentlich darlegen (können), wer für Cybervorfälle verantwortlich ist; dies wäre gerade zur Abwehr hybrider Bedrohungen, worunter auch Desinformation fällt, von Belang. Maßnahmen im Rahmen der Cyber Diplomacy Toolbox erfordern nicht in jedem Fall eine rechtlich abgesicherte Attribution. Sie zielen vielmehr darauf ab, Cybervorfälle mit politisch-kommunikativen und technischen Mitteln abzu-

wehren. Der Mitteleinsatz soll je nach Konfliktsituation zugeschnitten werden können.

Darüber hinaus ist zu überlegen, wie die in der Toolbox vorgesehenen Maßnahmen bei einem Ausfall wichtiger Infrastrukturen so eingesetzt werden können, dass die Führungs-, Handlungs- und Funktionsfähigkeit erhalten bleibt. Einerseits sollten auf EU-Ebene EAD und Kommission in enger Kooperation darüber beraten, andererseits die EU mit den Mitgliedstaaten. Dieses Krisenmanagement existiert bislang als Blueprint und muss personell, finanziell und kompetenzrechtlich durch die Mitgliedstaaten unterfüttert werden.

Die EU-Staaten sollten anerkennen, dass die Digitalisierung die klassische Diplomatie insofern auf nationaler Ebene herausfordert, als sich die außenpolitische Rolle der EU-Kommission im Zuge der Umsetzung der EU-Digitalstrategie ändert: Ihre Rolle bekommt mehr Gewicht in der Cyberdiplomatie. Es ist die EU-Kommission, die die Mitgliedstaaten dazu drängt, in Bezug auf Spaltungsversuche von außen und innen wachsam zu sein. Diese Aufforderung zur Wachsamkeit bei ausländischen Direktinvestitionen bzw. bei der Übernahme strategischer Wirtschaftsgüter, gerade in der Digitalwirtschaft, durch Drittstaaten könnte sogar noch stärker die Risiken berücksichtigen, die durch die Volatilität oder die Unterbewertung der europäischen Aktienmärkte entstehen.

Die demokratische Dimension

Die digitale Außenpolitik bzw. Cyberdiplomatie muss stärker als klassische Außen- und Sicherheitspolitiken darauf achten, nichtstaatliche Interessengruppen und unabhängige Wissenschaftler in den Politikprozess einzubeziehen und dem Multistakeholder-Ansatz möglichst breite Geltung zu verleihen. Zwar ist die bisherige Praxis der Multistakeholder-Governance dafür kritisiert worden, von den großen Digitalkonzernen als Instrument der Globalisierung eigener Interessen und technischer Standards missbraucht worden zu sein. Die maßgebliche Integration aller gesellschaftlichen Stakeholder hat sich aber im Endeffekt als grundrechtswahrender Faktor erwiesen. Besonders eine Reform der globalen Kooperationsinfrastruktur ist so nötig wie wichtig, wobei die ›demokratische‹ Dimension gestärkt werden muss, etwa indem die Rolle des Internet Governance Forum (IGF) als globales Stakeholdertreffen ausgebaut wird, Parlamentsvertreter konsequent an IGF-Treffen beteiligt und lokale wie regionale Initiativen miteinbezogen werden. In diesem Rahmen wird die EU-Cyberaußenpolitik, mandatiert durch die Mitgliedstaaten, weiter darauf hinarbeiten können, dass zentrale Institutionen wie die Internet Corporation for Assigned Names and Numbers (ICANN) und die Internet Engineering Task Force (IETF) auf Inklusivität und Partizipation aller gesellschaftlichen Gruppen ausgerichtet werden und nicht nur auf die Interessen der Wirtschaft (vgl. SWP-Studie 12/2019). Gerade parlamentarische Expertise ist hier gefragt, wie sie zuletzt in den Internet Governance Foren zunehmend genutzt wurde.

Die technologieinduzierte Verunsicherung in der globalen Politik schlägt sich auf allen Ebenen deutlich in einer grundlegend veränderten Wahrnehmung der Chancen und Gefahren zwischenstaatlicher Interdependenz nieder. Die US-amerikanischen Politologen Henry Farrell und Abraham L. Newman weisen darauf hin, dass Interdependenz nicht nur Versprechen, sondern auch Gefahr sei (*International Security*, Juli 2019). Globale Netzwerke und Lieferketten im Finanz- und Handelssystem, in der Verwaltung des Internets und der globalen Kommunikationsordnung seien stark asymmetrisch geprägt und könnten von mächtigen Staaten als Waffe gegenüber politischen Gegnern verwendet werden. Die Corona-Pandemie und das selbstbewusste Auftreten amerikanischer und chinesischer Internetkonzerne haben diesen Eindruck wirkmächtig werden lassen. In vielen Fragen, angefangen beim Zugang zum Weltwährungssystem und zu innovativer Technologie bis hin zu benötigten Medikamenten und digitaler Kommunikations- und Netz-

infrastruktur, bilden von privaten Akteuren kontrollierte Foren, Podien und Lieferketten eine Machtressource. Staaten sehen sich derzeit überfordert, wenn ihren Präsidenten von Digital-CEOs ihre virtuellen Megaphone entzogen werden können.

Die Revitalisierung der bilateralen Cyberdiplomatie in Form eines Handels- und Technologierats zwischen der EU und den USA nimmt vor diesem Hintergrund seit der Wahl Bidens zum US-Präsidenten eine besondere Stellung für die transatlantische Zusammenarbeit ein. Jede Neuaufstellung einer europäischen Cyberaußen- und Sicherheitspolitik soll aus US-Perspektive auf einer Allianz der demokratischen Multilateralisten gründen, die die USA miteinbeziehen muss. Nur zusammen mit Kanada, Australien, Japan, den USA und anderen vielleicht auch nur kurzfristig kooperierenden Staaten (Ad-hoc-Koalitionen) wird Europa stark genug sein, um sich langfristig gegen China und andere autoritäre Staaten behaupten zu können.

Hierzu finden sich in der Literatur bereits konkrete Vorschläge mit teilweise weitreichenden Konsequenzen. In der *Foreign Affairs* plädieren Richard A. Clarke und Rob Knake bereits im Oktober 2019 für die Gründung einer von den USA geführten »Internet Freedom League«, die alle diejenigen Staaten umfassen solle, die sich für ein freies, offenes und demokratisches Internet einsetzten. Sie sollte analog zum europäischen Schengenraum einen digitalen Block bilden, innerhalb dessen Daten, Dienstleistungen und Produkte sich frei bewegen könnten, während alle diejenigen Staaten, die die Meinungsfreiheit und den Schutz von Privatheit nicht achteten sowie Cyberkriminalität zuließen, ausgeschlossen wären: »The goal should be a digital version of the Schengen Agreement.« In diesem nach US-amerikanischer Sichtweise noch auszugestaltenden Cyber- und Informationsraum würden — angelehnt an die Koordinierung globaler Gesundheitspolitik durch die Weltgesundheitsorganisation — verletzliche Online-Systeme identifiziert werden, ihre Betreiber informiert und gemeinsam an deren Resilienz gearbeitet; Schadsoftware und Botnets würden frühzeitig beseitigt; Cyberangriffe unter den Mitgliedern wären untersagt. Freilich entsprechen diese Ziele im Wesentlichen den VN-Normen für verantwortungsvolles Staatenverhalten, gehen aber über diese hinaus. Eine derartige Allianz der Techdiplomacy sollte die verschiedenen Cybersicherheitsprogramme der EU in den westlichen Balkanstaaten und den sechs Ländern der Östlichen Partnerschaft in unmittelbarer Nachbarschaft der EU sowie in anderen Ländern weltweit einbinden.

Die wirtschaftlich-technologische Dimension

In seiner einflussreichen Studie zur Gefahr der Fragmentierung des globalen Internets beschreibt der Politologe Milton L. Mueller eindringlich, dass alle Hoffnungen auf ein globales Internet direkt davon abhingen, dass nichtstaatliche Akteure auch weiterhin eine wesentliche Rolle in seiner Governance innehätten. Es gebe keine Garantie dafür, dass einzelne europäische Mitgliedstaaten die von Russland und China betriebenen Maßnahmen der Internetzensur mithilfe von »Deep Packet Inspection«-Instrumenten und des Verbots von VPNs nicht imitierten, wenn ihnen kein starkes gesellschaftliches und rechtliches Korrektiv gegenübergestellt werde. Dieses Korrektiv kann kognitiv wie machtpolitisch wirken. In der EU-Kommission ist zur Vorbereitung einschlägiger Rechtsakte zu digitalen Märkten, Diensten, Algorithmen und Daten eine — in Abgrenzung zu amerikanischen, chinesischen und russischen Normierungen — herausragende Fachkompetenz aufgebaut worden. Dieses Wissen über Regulierung, Standards und Normen wird stark nachgefragt von diversen internationalen Akteuren wie der Afrikanischen Union, den Asean-Staaten, Brasilien, Australien oder Südkorea.

Europas Rolle als Normenexporteur in der Daten-, Informations- und Cybersicherheit hat überdies wirtschaftliche Folgen für Akteure auf dem internationalen Markt, die weiterhin im Binnenmarkt tätig sein wollen — trotz der hohen Anforderungen etwa zur Einhaltung von Standardvertragsklauseln

beim Datentransfer, die durch die restriktive Rechtsprechung des Europäischen Gerichtshofs im Juli 2020 noch verschärft wurden. Die Cyberdiplomatie der EU muss die künftigen weltweiten Standardvertragsklauseln zum Datentransfer sowie ein neues transatlantisches Privacy Shield mit den USA im gemeinsamen Rat für Handel und Technologie aushandeln.

EU-Ansätze zur Administration kritischer Internetressourcen werden in Zukunft noch striktere Ziele als bisher ins Auge fassen: Abhängigkeiten von einzelnen Lieferanten sollen diversifiziert werden. Die Auditierung durch ein EU-weites IT-Sicherheitskennzeichen soll den Marktzugang für alle Marktteilnehmer an Minimalstandards und Zertifizierungen knüpfen. Verschlüsselungstechnologien sollen zukünftig hohe europäische Sicherheitsstandards gewährleisten, um die Integrität und Sicherheit von Daten zu garantieren. Entschlüsselungspflichten oder Generalschlüssel für Strafverfolgungsbehörden, wie sie einzelne Regierungen fordern, werden indes von Zivilgesellschaft und Wirtschaft kritisch beurteilt.

Eine für die Sicherung europäischer Datenhoheit wichtige Initiative ist die Stärkung des europäischen Cloud- und Dateninfrastrukturprojekts GAIA-X. Um sich gegen die außereuropäische Marktmacht zu behaupten, versuchen führende Mitgliedstaaten und die EU-Kommission europäische Unternehmen zu bündeln und die eigenen Werte als Standortvorteil gegenüber Dritten auszuspielen. Datenschutz und Privatsphäre sollen nicht länger als Hemmschuh technologischer Entwicklung, sondern als Treiber von Innovation angesehen werden — gerade vor dem Hintergrund, dass Quantencomputing bereits heute noch gängige Methoden der Kryptographie umgehen kann.

Europäische Souveränität ist komplex, bedeutet aber im Umkehrschluss nicht, nun alles autark über die EU vorzunehmen, sondern eine technisch anspruchsvolle strategische Auswahl zu treffen, um jene Komponenten zu kontrollieren, die wirklich kritisch sind. Cyberdiplomatie des EAD in enger Absprache mit der EU-Kommission setzt eine intensive Partnerschaft zwischen öffentlichen und privaten Akteuren voraus, wenn sie technisch konkurrenzfähig sein will. Daher sollte sie anstreben, die Entwicklung von vertrauenswürdiger IT durch diese Partnerschaften zu befördern. Künstliche Intelligenz kann assoziativ zum Einsatz kommen, zur Früherkennung von Angriffen auf automatisierte Systeme. Schließlich müssen Informationen über Indicators of Compromise (IoC), also Merkmale und Daten, die auf Kompromittierung eines Systems oder Netzwerks hindeuten, allen Beteiligten zur Verfügung gestellt werden, sodass jeder an den angebotenen Lösungen teilhaben kann.

Die Cyberdiplomatie des EAD in Kooperation mit der Kommission bzw. der Agentur für Cybersicherheit (ENISA) sollte in die Lage versetzt werden, diese technologischen Voraussetzungen auf die Ebene der europäischen Infrastrukturen zu heben, damit Wirtschaft und KRITIS von den Ergebnissen profitieren können. Nicht zuletzt beabsichtigt die Kommission den KRITIS-Bereich zu erweitern. Neben den klassischen Sektoren wie Energie werden auch Institutionen im nationalen und strategischen Interesse in den Blick genommen. Künftig kommt der Kommission eine noch größere Rolle zu, wenn es darum geht, Verfügbarkeit, Integrität und Vertraulichkeit europäischer Daten durch eine Binnenmarktaußenpolitik sicherzustellen.

Update der Cyberdiplomatie nötig

Eine zusammenwachsende Welt braucht gemeinsame Regeln und einen verbindlichen Rechtsrahmen, damit sich gemeinsame Märkte entwickeln und das Sicherheitsdilemma abbauen kann. Die Nachkriegszeit wird nur dann nicht zur digitalen Vorkriegszeit werden, wenn sich die EU-Mitgliedstaaten einer Cyberdiplomatie zuwenden, die in ihrer institutionellen, demokratischen und wirtschaftlichen Dimension an der Maxime der »strategischen Offenheit« orientiert ist. Letztere ist für die Aufrechterhaltung des Binnenmarktes zentral, um den Sirenengesängen merkantilistischer

Abschottung und territorialen Souveränitätsdenkens auch im digitalen Zeitalter wirksam begegnen zu können. Die digitale Selbstbehauptung der EU manifestiert sich darin, dass Abhängigkeiten reduziert, die Stärkung der Rechte von Bürgern gefördert, Plattformen zur Rechenschaft gezogen und die Wettbewerbsfähigkeit der europäischen Wirtschaft gesteigert wird.

Mit diesem Anspruch vor Augen sollte die EU-Cyberdiplomatie *erstens* dazu beitragen, dass Bürger die Selbstbestimmung über ihre persönlichen Daten behalten. *Zweitens* ist Cyberdiplomatie im Dienste der digitalen Souveränität der EU mit strategischer Handlungsfähigkeit verbunden und setzt voraus, dass die Union ihre Vorstellungen von Datenschutz und -sicherheit auch international durchsetzen kann. Eine europäische »Resouveränisierung« der Cyberdiplomatie im digitalen Zeitalter meint *drittens* die Einsicht, dass ein Mindestmaß an Herrschaft bzw. Kontrolle über die notwendigerweise genutzten technologischen Ressourcen — von Internetknotenpunkten über Cloud-Infrastruktur bis hin zur internationalen Standardsetzung — die digitale Souveränität überhaupt erst möglich macht. Dazu gehört *viertens* die Überprüfbarkeit von Recht und Politik der Digitalität vor der europäischen Gerichtsbarkeit. China und die USA beschränken sich zum Beispiel bei der kritischen Infrastruktur (Hard- und Software) aus Gründen der Cybersicherheit im Wesentlichen auf einheimische Anbieter. *Fünftens* wäre im Sinne der Reziprozität und Wettbewerbsfähigkeit eine Harmonisierung von IT-Sicherheitsgesetzgebung sowie von Beschaffungs- und Zulassungsregeln auf EU-Ebene folgerichtig. Eine Zusammenarbeit der EU mit Demokratien wie USA, Kanada, Singapur, Südkorea oder Taiwan könnte dies begünstigen.

Diesen Zielen dienen die neuen und geplanten Rechtsakte und Strategien der EU zu Daten, Märkten, Diensten und Algorithmen in Europa und zuletzt zur Cybersicherheit. Wenn die Union dergestalt voranschreitet, sollten die Mitgliedstaaten auch bereit sein, das machtpolitische Narrativ Europas im digitalen Zeitalter einem Update zu unterziehen, und zwar mittels einer robusteren, besser aufeinander abgestimmten Außen-, Sicherheits- und Verteidigungspolitik und indem seine strategische Ausrichtung und institutionelle Verankerung in der EU-Cyberdiplomatie gewürdigt wird. Das wäre zumindest die logische Konsequenz. Vonnöten sind sicherlich qualifizierte Mehrheitsentscheidungen, um im Fall schwerwiegender Cyberangriffe mit restriktiven Maßnahmen reagieren zu können.

Aber nicht immer ist Harmonisierung der Weg zur Optimierung. Ein gesamteuropäischer und gesamtgesellschaftlicher Ansatz in der Cybersicherheit meint die Formalisierung des Wissensaustauschs zwischen Organen, Sicherheitsbehörden, der Wissenschaft und Wirtschaft. Verteidigung und Diplomatie im Cyber- und Informationsraum bleiben hoheitliche Aufgaben. Spätestens seit dem Urteil des Bundesverfassungsgerichts (BVerfG) zum Bundesnachrichtendienst vom 19. Mai 2020 und dem Nichtannahmebeschluss des BVerfG vom 16. Dezember 2020 ist klar, dass die rechtsstaatlichen Verpflichtungen aller deutschen Behörden nicht an der staatlichen Außengrenze enden und dass der Staat grundsätzlich für Verletzungen von Grundrechten im Ausland haftet — dies gilt auch im CIR. Das heißt, eine enge Zusammenarbeit in dieser komplexen Cybersicherheitsarchitektur ist geboten. Zugleich stellt sie in Deutschland neue Anforderungen an Verfassungsprinzipien wie das Trennungsgebot oder den Einsatz des Militärs im Innern. Cyberdiplomatie sollte darauf aufbauen können, das Cybersicherheit auf nationaler Ebene Bedingungen schafft, um Amtshilfe im europäischen Kontext und mit Allianzpartnern rechtssicher zu ermöglichen.

Dr. Annegret Bendiek ist Stellvertretende Leiterin der Forschungsgruppe EU/Europa.
PD Dr. Matthias C. Kettemann, LL.M. (Harvard), ist Forschungsprogrammleiter am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) und Forschungsgruppenleiter am Humboldt Institut für Internet und Gesellschaft und am Sustainable Computing Lab der Wirtschaftsuniversität Wien.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364
doi: 10.18449/2021A12