SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Die EU als Friedensmacht in der internationalen Cyberdiplomatie

Annegret Bendiek

Seit Cyberangriffe auf Computernetzwerke europäischer Verteidigungs- und Außenministerien öffentlich bekanntgeworden sind, fordern Sicherheitspolitiker, dass die EU eine ausreichende Cyberabwehr und Cyberrückschlagfähigkeiten entwickeln muss. Nach wie vor setzt die EU in der Cybersicherheit jedoch auf Cyberdiplomatie und versucht sich auf diese Weise als Friedensmacht zu positionieren. Ihr Diplomatischer Reaktionsrahmen, verabschiedet im Oktober 2017, sieht hauptsächlich nichtmilitärische Instrumente zur Gefahrenabwehr vor. Europa wäre gut beraten, sich angesichts wachsender Herausforderungen an den Stufenplan der Cyberdiplomatie zu halten, der auf dem Prinzip der Sorgfaltsverantwortung fußt.

Cyberangriffe wie jene auf das Computernetz der Bundesregierung legen nicht nur einzelne Infrastrukturen lahm, sondern können auch Teil hybrider Kriegsführung sein. Dabei bezeichnet »hybrid« die absichtliche, verdeckte oder offene Verwendung ziviler und militärischer Instrumente durch staatliche oder nichtstaatliche Akteure. Neben Cyberangriffen gehören hierzu Desinformationskampagnen, Spionage, wirtschaftlicher Druck, der Einsatz von Stellvertreterkräften oder andere subversive Tätigkeiten. Nach dem Giftgasanschlag in London haben die Staats- und Regierungschefs der EU Ende März 2018 ihre uneingeschränkte Solidarität mit Großbritannien erklärt und Russland Konsequenzen angedroht. Erwogen werden weitere Sanktionen, aber auch ein digitaler Gegenschlag (Hackback).

Cyberabwehr: defensiv oder offensiv?

Politisch ist umstritten, ob angegriffene Staaten offensive Gegenmaßnahmen wie etwa Hackbacks ergreifen sollen, um die Quelle eines Cyberangriffs neutralisieren zu können. Die deutsche Cybersicherheitsstrategie von 2016 ist der defensiven Cyberverteidigung verpflichtet. Damit in Einklang vertritt die Bundesregierung die Position, dass der Staat militärische und strategische Cyberwaffen sowie eine Rechtsgrundlage für ihren Einsatz benötigt, um Angriffe wie 2015 auf den Deutschen Bundestag oder seit 2016 auf das Regierungsnetz ahnden zu können. Für die Nato gelten Attacken im Cyberraum seit 2016 als Art der Kriegsführung, die einen Aufruf zur kollektiven Verteidigung nach Artikel 5 des Nordatlantikvertrags nach sich ziehen kann. In der Alli-

Dr. Annegret Bendiek ist Wissenschaftlerin in der Forschungsgruppe EU/Europa

anz wird diskutiert, ob offensive Computernetzwerkoperationen ihrer Mitgliedstaaten Bestandteil der Operationsplanung sein sollen. Seit dem Warschauer Nato-Gipfel 2016 wurde die Zusammenarbeit zwischen Nato und EU durch Informationsaustausch und gemeinsame Cybersicherheitsübungen verstärkt. Mit seinem Weißbuch 2016 zur Sicherheitspolitik griff das Bundesverteidigungsministerium diese Entwicklung auf und schuf einen sechsten militärischen Organisationsbereich, den Bereich Cyber- und Informationsraum mit zunächst rund 13 500 Dienstposten. Für den Fall der Selbst- und Bündnisverteidigung dürfen defensive und offensive Cyberabwehrfähigkeiten vorgehalten werden. Strittig ist, ob dies auch in Friedenszeiten für offensive Fähigkeiten gilt. Die Proliferation von Schadsoftware für Cyberangriffe rechtfertige Kritikern zufolge nicht die kurzfristigen Vorteile des angeblich größeren Abschreckungspotentials. Daher fordern sie, vertrauens- und sicherheitsbildende Maßnahmen sowie Rüstungskontrolle durch Vereinte Nationen (VN) und OSZE zu forcieren. Der Aufbau offensiver Cyberverteidigungsfähigkeiten drohe die wechselseitige Unsicherheit zu erhöhen und Konflikte anzuheizen. Nur eine längerfristige, europäisch abgestimmte Cyberdiplomatie könne helfen, Sicherheit in Europa herzustellen und Eskalationsspiralen zu vermeiden. Aus wohlverstandenem Eigeninteresse positioniert sich die EU in der Cybersicherheitspolitik als Friedensmacht, die auf Ausgleich und Verständigung setzt.

Formate der Cyberdiplomatie

Im Gegensatz zur Cyberverteidigung bietet die Cyberdiplomatie Möglichkeiten der Konfliktdeeskalation und damit des Aufbaus einer Friedensmacht. Mittlerweile gibt es in mehr als 30 Staaten Beauftragte für Cyberaußenpolitik. Dänemark hat sogar einen eigenen Botschafter für Cyberdiplomatie ernannt. Im weitesten Sinne umfasst sie vertrauens- und sicherheitsbildende Maßnahmen. Zu ihr gehören Aspekte der internationalen Normenbildung, des Datenschutzes und der Meinungsfreiheit, der Infrastruktur des Internets sowie der Strafverfolgung im Rahmen internationaler Rechtshilfeabkommen. Viele Regierungen verfügen allerdings weder über das Wissen noch über die notwendigen Ressourcen, um grundlegende Cybersicherheitsstandards einzuhalten oder überhaupt festzustellen, welche Angriffe über Server auf ihrem Hoheitsgebiet laufen. Die Idee, eine zentrale globale Regulierungsinstanz für die Sicherheit im Cyberraum zu gründen, stößt jedoch bei den meisten Staaten auf massive Souveränitätsvorbehalte und dürfte bis auf weiteres unrealistisch sein. Sehr viel wahrscheinlicher ist die zunehmende Verregelung des Cyber- und Informationsraums. Eine Gruppe von 25 internationalen Regierungsexperten, die von der Generalversammlung der VN beauftragt war, erzielte 2015 einen Konsens darüber, dass internationales Recht auch im Cyberraum angewandt werden soll, einschließlich des Rechts auf Selbstverteidigung. Über die Einrichtung eines sogenannten Attributionsrats war sich die Gruppe 2017 allerdings uneinig. Attribution, also die eindeutige Identifizierung des Verursachers einer Cyberattacke, setzt den sensiblen Austausch von Informationen in IT-Notfallteams (CERT) und Geheimdiensten voraus.

Im bilateralen Rahmen haben die Präsidenten Xi Jinping und Wladimir Putin 2016 in Shanghai eine gemeinsame Erklärung über eine neue Phase der umfassenden strategischen Partnerschaft zwischen China und Russland unterzeichnet. Peking und Moskau äußerten sich besorgt, dass die Informations- und Telekommunikationstechniken für Einmischung in innere Angelegenheiten missbraucht würden. Die internationale Gemeinschaft solle auf Basis gegenseitigen Respekts und Nutzens sowie der Gerechtigkeit zusammenarbeiten und gemeinsam auf Bedrohungen der Informationssicherheit reagieren. Auch die USA setzen auf bilaterale Abkommen, etwa mit China, um Cyberkriminalität zu bekämpfen.

Seit dem Scheitern der multilateralen Verhandlungen auf VN-Ebene plädieren Cybersicherheitsexperten dafür, dass »Koalitionen der Willigen« aus G20- oder G7-Staaten die internationale Normenbildung vorantreiben. Im Aufwind sind Two-Track-Formate wie etwa die Global Commission on the Stability of Cyberspace. Die Attribution zu stärken ist nicht nur ein Anliegen der Staaten, sondern auch der Privatwirtschaft. Microsoft sprach sich im Februar 2017 für eine »digitale Genfer Konvention« aus. In die gleiche Richtung geht die jüngste Initiative »Charter of Trust«, die Siemens im Februar 2018 auf der Münchner Sicherheitskonferenz lancierte. Das Weltwirtschaftsforum schließlich will ein »Global Centre for Cybersecurity« gegen Cyberkriminalität schaffen und damit auch die Zusammenarbeit zwischen Privaten und Behörden verbessern.

Die Cyber-Außen- und Sicherheitspolitik der EU

Cybersicherheit ist nicht nur eine Aufgabe der Staaten, sondern auch der EU. Sie beschränkt sich nicht auf die Resilienz der Netzwerke, den digitalen Binnenmarkt und die Verfolgung von Cyberkriminellen, sondern erstreckt sich auch auf die Gemeinsame Außen- und Sicherheitspolitik (GASP) und die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) der EU (siehe Tabelle auf der folgenden Seite). Auf Unionsebene befasst sich mittlerweile eine ganze Reihe Akteure mit Cyber-Außen- und Sicherheitspolitik. Die wichtigsten sind die EU-Agentur für Netz- und Informationssicherheit (ENISA), das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) unter dem Dach von Europol, das EU-Zentrum für Informationsgewinnung und -analyse (INTCEN), die Abteilung Aufklärung des Militärstabs der EU (EUMS INT) und sein Lagezentrum (SITROOM), die bei INTCEN angesiedelte EU-Analyseeinheit für hybride Bedrohungen, das IT-Notfallteam für die Organe und Stellen der EU (CERT-EU) sowie das Zentrum der Europäischen Kommission für die Koordination von Notfallmaßnahmen (ERCC). Nicht zu vergessen sind die gemäß Richtlinie zur Netz- und Informationssicherheit (NIS) neu geschaffenen Strukturen und Mechanismen, etwa das Netz der IT-Noteinsatzteams der Mitgliedstaaten (CSIRTs).

Die Horizontale Gruppe »Fragen des Cyberraums« des Rates wurde 2015 ins Leben gerufen, um politische Aspekte des Cyberraums übergreifend im Rat zu koordinieren. Sie kann an legislativen wie auch nichtlegislativen Tätigkeiten mitwirken. Zudem haben die EU-Staaten im Februar 2015 beschlossen, die Cyberdiplomatie auf EU-Ebene im Europäischen Auswärtigen Dienst (EEAS) zu stärken. Bekräftigt wurde dies im November 2016 mit dem Implementierungsplan zur Sicherheit und Verteidigung. Wichtige Koordinierungsstellen strategischer Vorfeldanalyse für die GASP bilden der Arbeitsstab der Cyberdiplomacy, EU INTCEN für die zivile und EUMS INT für die militärische Lagebilderstellung. Um Cyberangriffe abzuwehren, zu rekonstruieren und die Verursacher zu ermitteln, sind Computerforensiker auf zahlreiche Quellen aus unterschiedlichen Staaten und Unternehmen angewiesen. Bei der Zusammenarbeit in diesem neuen Feld kann die EU auf eine eingespielte Kooperation zwischen Ministerien und Sicherheitsbehörden zurückgreifen. Für die Terrorismusbekämpfung gelten Sonderregelungen. Eine europäisch koordinierte Politik zwischen verbindlichem Informationsaustausch auf der einen, Überwachung und Nutzung geteilter Informationen auf der anderen Seite ist bisher jedoch keine vertraglich verankerte EU-Kompetenz. Die erneuerte Cybersicherheitsstrategie der EU von September 2017 bietet Ansatzpunkte zur vertrauens- und sicherheitsbildenden Zusammenarbeit, aufbauend auf den vier Pfeilern der EU-Cybersicherheit (siehe Tabelle).

Erster Pfeiler: Um der wachsenden Gefahr grenzüberschreitender Cyberkriminalität zu begegnen, sollen Instrumente geschaffen werden, mit denen Täter wirkungsvoller verfolgt werden können. Derzeit wird über

Tabelle
Cybersicherheit in der EU: Zuständigkeitsbereiche

	Frieden, Sicherheit, Justiz	*Binnenmarkt*	*GSVP: Cyberverteidigung*	*GASP: Cyberdiplomatie*
EU	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT-Netzwerk CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU-Hybrid Fusion Cell ERCC
National	Exekutiv- und Datenschutzbehörden	Für die NIS zuständige Behörden Nationale CSIRTs	Verteidigungs-, Militär- und Sicherheitsbehörden	Außenministerien

CERT: Computer Emergency Response Team, *CSIRT*: Computer Security Incident Response Team, *EC3*: European Cybercrime Centre, *EDA*: European Defence Agency, *EEAS*: European External Action Service, *ENISA*: European Union Agency for Network and Information Security, *ERCC*: Emergency Response Coordination Centre, *EU INTCEN*: European Union Intelligence and Situation Centre, *EU-LISA*: European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice, *EU SITROOM*: European Union Situation Room, *EUMS INT*: European Union Military Staff, Intelligence Directorate Mission, *GSA*: European Global Navigation Satellite Systems Agency, *NIS*: Network and Information Security, *SIAC*: Single Intelligence Analysis Capacity.

eine »E-Evidence«-Richtlinie verhandelt, die den grenzüberschreitenden Zugang zu elektronischen Beweismitteln erleichtern soll. Ebenfalls im Gespräch ist eine Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln wie Bitcoin. Sie soll die Zusammenarbeit zwischen Strafjustizbehörden verbessern.

Zweiter Pfeiler: Die ENISA wird aufgewertet, indem ihr Personal von rund 80 auf 125 Mitarbeiter und ihr Jahresetat von 11 auf 23 Millionen Euro aufgestockt wird. Die Agentur soll jährliche gesamteuropäische Cybersicherheitsübungen organisieren und die Kooperation zwischen IT-Noteinsatzteams der Mitgliedstaaten (CSIRTs) steuern. Schon früher wurden diese Übungen gelegentlich auf verbündete Nicht-EU-Staaten ausgeweitet. Vor allem soll die ENISA Einrichtung und Umsetzung eines EU-weiten Zertifizierungsrahmens begleiten. Ziel ist es, IT-Produkte und -Dienstleistungen durch Marktanreize sicherer zu machen und Nutzer in die Lage zu versetzen, fundierte Kaufentscheidungen zu treffen. Voneinander abweichende Zertifizierungssysteme sollen harmonisiert werden, um den digitalen Binnenmarkt für vertrauenswürdigere Produkte zu stärken. Diese Maßnahme geht auf die Netz- und Informationssicherheitsrichtlinie (NIS-Richtlinie) zurück, die im Mai 2018 in Kraft treten wird. Die EU-Regulierung dient als Referenz, um ähnliche Verbesserungen auch im OSZE-Raum zu erreichen.

Dritter Pfeiler: Im Dezember 2017 haben die 25 Verteidigungsminister der EU die Ständige Strukturierte Zusammenarbeit (PESCO) beschlossen. Zwei der 17 Projekte sind ausdrücklich Europas Cybersicherheit gewidmet. Bei den anderen geht es Berichten zufolge auch um die Standardisierung von Soldatensystemen, also der elektronischen Ausrüstung, der Sprach- und Datenkommunikation oder der Software. Griechenland will ein europäisches IT-Notfallteam, Litauen federführend eine europäische Cyberabwehr aufbauen. Es soll ein »Cyber-Schengenraum« geschaffen werden, um die über alle Grenzen hinweg agierende Online-Kriminalität zu bekämpfen. Bis Ende 2020 will die Europäische Investitionsbank mehr als 6 Milliarden Euro in die Entwicklung sogenannter Dual-Use-Technologie für Cybersicherheit und zivile Sicherheit investieren.

Vierter Pfeiler: Die EU und die Regierungen ihrer Mitgliedstaaten unterhalten jeweils bilaterale Cyberdialoge. Gemäß der Cybersicherheitsreform vom September 2017 schlägt die EU vor, einen strategischen Rahmen für die internationale Zusammenarbeit in Cyberabwehr und Konfliktprävention auszuarbeiten. Als erster Schritt wurden die GASP-Instrumente sowie die Dual-Use-Verordnung für Exportkontrollen von Gütern mit doppeltem Verwendungszweck aktualisiert.

Diplomatischer Reaktionsrahmen

Die Zunahme von Cyberattacken nötigt internationale Akteure zu Überlegungen, wie darauf angemessen zu antworten wäre. So verhängte die Obama-Administration zum ersten Mal 2014 einseitige Sanktionen, nachdem ein amerikanisches Tochterunternehmen des Sony-Konzerns Opfer eines verheerenden Cyberangriffs geworden war, bei dem alle Unternehmensdaten kopiert wurden. Zwei Jahre später reagierte Washington ähnlich, als im großen Stil Personaldaten der US-Administration infolge einer Cyberattacke abgeflossen waren. Wegen der mutmaßlichen russischen Einmischung in den US-Wahlkampf 2016 belegte die US-Regierung im März 2018 fünf Firmen und Organisationen sowie 19 Einzelpersonen mit Sanktionen, als Antwort auf »böswillige russische Cyberaktivitäten«. Die EU wiederum wies im Februar 2015 erstmals auf die Notwendigkeit einer gemeinsamen Cyberdiplomatie hin. Im Juni 2017 schlug sie vor, einen »Cyberwerkzeugkasten« (Cyber Diplomacy Toolbox) für eine gemeinsame diplomatische Antwort der Union auf böswillige Cyberaktivitäten zu schaffen. Auf diese Weise wollte die EU vor allem die außen- und sicherheitspolitische Reaktionsfähigkeit unterhalb der Schwelle zum bewaffneten Konflikt gewährleisten. Damit würde sie ihre Bestrebungen ergänzen, gemäß NIS-Richtlinie Mindeststandards und Meldepflichten durchzusetzen sowie resiliente Informations- und Kommunikationssysteme im digitalen Binnenmarkt aufzubauen. Der Cyberdiplomatie-Ansatz als Reaktion auf Anschläge soll auf EU-Ebene zuvorderst die politischen Maßnahmen der GASP, darunter auch restriktive, zum Tragen bringen. Im Oktober 2017 wurde der geplante Cyberwerkzeugkasten unter der neuen Bezeichnung »Diplomatischer Reaktionsrahmen« verabschiedet. Er soll die Zusammenarbeit bei der Eindämmung unmittelbarer und langfristiger Bedrohungen erleichtern und helfen, langfristig auf das Verhalten von Tätern und potentiellen Angreifern einzuwirken. Die Reichweite einzelstaatlichen Handelns sei zu gering, um Kosten-Nutzen-Logiken von Angreifern beeinflussen zu können. Demgegenüber kann die EU-Diplomatie mit ihren Sanktions- und Regulationsmöglichkeiten einen strategischen Mehrwert bieten. Dabei verpflichtet sie sich auf die internationalen Prinzipien zur Einhaltung von Sorgfaltspflichten im Cyberraum und beabsichtigt, im Austausch mit Drittstaaten die Cyberdiplomatie zu stärken, um Cyberangriffe zu bekämpfen. Die Gruppe der Regierungsexperten auf VN-Ebene (GGE) hat den Grundsatz der Einhaltung von Sorgfaltspflichten in ihren Abschlussbericht vom Juni 2015 aufgenommen. Staaten sollen demnach sicherstellen, dass ihr Hoheitsgebiet und damit vor allem dort befindliche oder sonst unter ihrer Kontrolle stehende Computersysteme und Infrastruktur nicht zu Angriffen auf die Infrastruktur anderer Staaten missbraucht werden.

Fünf Kategorien von Maßnahmen

Die EU kann in der Cyberdiplomatie auf den Instrumentenkasten der GASP zurückgreifen. Zu unterscheiden sind präventive, kooperative, stabilisierende und restriktive Maßnahmen sowie völkerrechtskonforme Strafmaßnahmen zur Selbstverteidigung. Während politische Maßnahmen auf EU-Ratsebene mit Hilfe des Europäischen Auswärtigen Dienstes getroffen werden, sind völkerrechtskonforme Strafmaßnahmen souveräne Entscheidungen der Staaten.

Prävention: Im Zuge der politischen Dialoge mit Drittstaaten wurden Cyberdialoge

entwickelt, um durch Informationsaustausch und verstärkte Zusammenarbeit das Verhalten und die Positionierung der Dialogpartner zu beeinflussen. Besonders wichtig sind die Dialoge mit Regionalorganisationen wie der Afrikanischen Union. Wie sich in diesen Regionen Fähigkeiten für den Umgang mit dem Cyberraum aufbauen lassen (Cyber Capacity Building), wird in Assoziierungs-, Partnerschafts- und Kooperationsabkommen oder auch Gemeinsamen Erklärungen zwischen der EU und den betreffenden Regionalorganisationen festgelegt.

Kooperation: Eine EU-Delegation in einem Gastland kann eine diplomatische Note (Demarche) an das betreffende Land richten. Dafür ist eine Weisung des Hohen Vertreters der EU für Außen- und Sicherheitspolitik nötig. Der Delegationsleiter kann im Konfliktfall einen ausführlichen Gesprächsführungsvorschlag oder lediglich Kernaussagen übermitteln. Demarchen können auch zusammen mit Drittstaaten formuliert und übergeben werden. Ist der EU-Delegationsleiter im Konfliktfall zurückgerufen worden, entfällt dieser Weg kooperativer Konfliktlösung.

Stabilisierung: Der Europäische Rat kann eine Aktion oder einen Standpunkt der EU festlegen, muss dafür aber einstimmig entscheiden. Er kann auch einen Beschluss zur Umsetzung einer solchen Aktion fassen. In diesem Falle reicht die qualifizierte Mehrheit aus, allerdings nicht bei Umsetzungsakten mit militärischen oder verteidigungspolitischen Bezügen (Artikel 31 Absatz 2 EUV). Bisher wurde nicht versucht, mit einer häufigeren Anwendung von Umsetzungsakten das Prinzip der qualifizierten Mehrheit in die GASP einzuführen. Ferner kann die Hohe Vertreterin der EU für Außen- und Sicherheitspolitik »im Namen der EU« eine Erklärung abgeben. Diese muss aber mit allen EU-Staaten abgestimmt sein. Eine solche Erklärung ergeht meist dann, wenn eine sofortige Reaktion nicht notwendig ist, wenn die EU erst eine Position zu einer neuen Situation erarbeiten muss oder wenn sie eine etablierte Position angepasst hat. Die Hohe Vertreterin kann aber auch in eigener Verantwortung eine Erklärung abgeben, wenn eine schnelle Reaktion erforderlich, aber eine Abstimmung im Kreis der EU-27 nicht möglich ist.

Restriktionen: Die EU kann restriktive Maßnahmen (Sanktionen) verhängen, wenn sie politische Ziele infolge schwerwiegender Cyberangriffe durchsetzen will. Diese Maßnahmen richten sich in der Regel gegen Vertreter von Regierungen bestimmter Drittstaaten, aber auch gegen Staatsunternehmen oder andere juristische und natürliche Personen. Sanktionen müssen vom Rat einstimmig beschlossen werden und im Einklang mit den Zielen der GASP gemäß Artikel 24 EUV stehen. Grundsätzlich wird unterschieden zwischen Sanktionen, die die EU autonom beschließt, und solchen, die sie gemäß Beschluss des Sicherheitsrats der Vereinten Nationen zu verhängen verpflichtet ist. In der EU gilt das Gebot, dass Sanktionen gezielt sein müssen (targeted sanctions). Zum Beispiel können bestimmte Personen oder Firmen auf eine Sanktionsliste gesetzt werden, um ihre Konten sperren zu können. Allerdings müssen rechtsstaatliche Mindeststandards gegenüber den Betroffenen erfüllt sein. Dafür wurden sogenannte Rechtmäßigkeitsvoraussetzungen formuliert, etwa dass den Betroffenen die Gründe für ihre Listung und die Möglichkeit zur Klage mitgeteilt werden müssen.

Völkerrechtskonforme Reaktionen: Mit dem Vertrag von Lissabon wurden die Solidaritäts- und die Beistandsklausel eingeführt. Beide können bei schwerwiegenden Cyberangriffen angewandt werden. Die Solidaritätsklausel nach Artikel 222 AEUV sieht vor, dass sich die Staaten der EU gegenseitig unterstützen, wenn einer oder mehrere von Terroranschlägen, Naturkatastrophen oder von Menschen verursachten Katastrophen (und damit auch schwerwiegenden Cybervorfällen) betroffen sind. Die Beistandsklausel nach Artikel 42 Absatz 7 EUV entspricht in etwa Artikel 5 des Nato-Vertrags, der jedoch für Nato-Mitglieder Vorrang hat. Zum ersten Mal wurde die Beistandsklausel im November 2015 von Frankreich nach

den Terroranschlägen von Paris in Anspruch genommen. Laut dem Diplomatischen Reaktionsrahmen der EU vom Oktober 2017 erforden völkerrechtskonforme Reaktionen keine eindeutige Attribution von Herkunft und Verursacher von Cyberattacken. Diese Lesart entspricht den Auslegungen internationaler Rechtsexperten, festgehalten im Tallinn-2-Manual zur Anwendung internationalen Rechts im Cyberraum.

Exportkontrollen

Die EU unterstützt ihre Cyberdiplomatie und ihren Anspruch auf Sorgfaltsverantwortung auch dadurch, dass sie den Export von Gütern mit doppeltem Verwendungszweck strenger kontrollieren lassen will. Die Dual-Use-Verordnung vom Mai 2009 regelt gemeinsame Genehmigungspflichten aller Mitgliedstaaten bei Ausfuhr, Vermittlung und Durchfuhr solcher Güter. Mitte Dezember 2017 hat die Europäische Kommission eine Neufassung der Anhänge I, IIa bis IIg und IV der Verordnung veröffentlicht. Inhaltlich umfasst die Aktualisierung vor allem neue Kontrollen für bestimmte Güter, etwa für IT-Hardware. Die Einstufung von Gütern als kontrollpflichtig (Anhang I) orientiert sich zum einen an Vorgaben internationaler Verträge und Verpflichtungen, vor allem der Resolution 1540 des VN-Sicherheitsrats, der Chemiewaffenkonvention und der Biowaffenkonvention. Zum anderen richtet sie sich nach Kontrolllisten internationaler multilateraler Exportkontrollregime, vorrangig des Wassenaar-Abkommens, der Nuclear Suppliers Group, der Australischen Gruppe sowie des Missile Technology Control Regime (MTCR). Besonders diese Listen unterliegen stetigen Änderungen. Nicht nur ist die Ausfuhr bestimmter Güter in sanktionierte Staaten verschärfter Kontrolle unterworfen. In vielen Fällen muss auch eine gesonderte Genehmigung für den Export von Dual-Use-Gütern beantragt werden. Bei Nichtbeachtung drohen empfindliche Straf- und Bußgelder.

Sorgfaltsverantwortung als Stufenplan

Der Zwang, einstimmig zu entscheiden, macht es der EU schwer, sich als Friedensmacht im Cyberraum zu profilieren. Die Staaten der Union weisen nicht nur große strategische Ambivalenzen auf, etwa in der Russlandpolitik. Auch die Kohärenz im auswärtigen Handeln lässt zu wünschen übrig. Der Anspruch der EU, als Friedensmacht zu wirken, kommt dadurch zum Ausdruck, dass ihre Mitgliedstaaten das »Due Diligence«-Prinzip durch die politischen GASP-Instrumente zu stärken suchen. »Due Diligence« wird in völkerrechtlichen Abhandlungen meist mit dem nicht unproblematischen Begriff Sorgfaltspflicht übersetzt. Dieser umfasst jedoch lediglich Restriktionen eigenen Handelns für den Fall, dass es einem selbst schadet. Dagegen enthält der Terminus Sorgfaltsverantwortung eine besondere normative Kraft. Sie speist sich aus der Idee, dass die EU nicht nur die Einhaltung von Regeln in ihrem eigenen Rechtsraum gewährleisten muss, sondern auch Verantwortung für die externen Auswirkungen ihres Handelns tragen soll, zum Beispiel durch eine strengere Exportpolitik. Europäische Entscheidungen greifen immer häufiger über den Rechtsraum der EU hinaus. Ihr allein obliegt es, hier für Kohärenz zu sorgen. Was den Schutz des Cyberraums anbelangt, sollten die Mitgliedstaaten sich nicht darauf beschränken, auf unverantwortliche, im Alleingang getroffene Entscheidungen zu verzichten. Darüber hinaus wären die Mitglieder der EU in die Pflicht zu nehmen, zusammen mit anderen Staaten alles von ihnen vernünftigerweise Erwartbare zu unternehmen, um ihren Beitrag zu einem »offenen, globalen, freien, friedlichen und sicheren Cyberraum« zu leisten.

Die Debatte ist im Gange, inwieweit EU-Regierungen sich sogar rüsten sollten, um technische Gegenmaßnahmen zu ergreifen oder gar Gegenschläge zu führen, wie es derzeit gegen Russland erwogen wird. Das wäre die höchste Eskalationsstufe nach der Beistandsklausel, soweit die Maßnahme ge-

mäß Sorgfaltspflicht in der EU abgestimmt ist. Die letzte Stufe des Krisenmanagements bestände darin, einen laufenden Angriff durch aktive Gegenwehr zu stoppen. Ultima ratio wäre ein sogenannter Hackback, also das gezielte Ausschalten eines Servers, von dem ein Angriff ausgeht. Im Sinne der Sorgfaltsverantwortung ist dies nur dann, wenn ein laufender Angriff schwere, existenzbedrohende Folgen hat und alle anderen Mittel erschöpft sind. Die dafür notwendigen rechtlichen Rahmenbedingungen und die Kompetenzverteilung sind noch nicht festgelegt, selbst auf nationaler Ebene nicht.

Wichtigste und dauerhaft wirksame Mittel der EU in diesem Kontext sind Prävention und Detektion. Prävention umfasst die Maßnahmen im Zuge der NIS-Richtlinie, wie die Einführung von Mindeststandards und Meldepflichten für Betreiber Kritischer Infrastrukturen. Provider von Telekommunikation dürfen bei Störungen den Datenverkehr analysieren und identifizierte Verursacher notfalls blockieren.

Detektion beinhaltet Aufklärung und Attribution von Angriffen. Maßgeblich ist hier die politische Bewertung. Sie muss das Gesamtbild der Vorfälle im Cyberraum berücksichtigen, weil mit militärisch relevanten hybriden Bedrohungen zu rechnen ist. Im Falle professioneller Angriffe ist Cyberdiplomatie unter gleichgesinnten Staaten erforderlich, um Analysen von Codefragmenten und Angriffsabläufen auf der Ebene der Sicherheitsbehörden auszutauschen. Dies gestattet oft Rückschlüsse auf Hackergruppen und deren Herkunft. Für einen vergleichbaren Austausch beim Schutz Kritischer Infrastruktur soll das CSIRT-Netz mit seinen technischen Kompetenzen sorgen. Cyberdiplomatie setzt überdies den Austausch zwischen Behörden und Wirtschaft voraus. Öffentliche und private CERT-Verbünde und Zusammenschlüsse in der Industrie sind unverzichtbar, wenn es darum geht, Expertenwissen auch in der Cyberdiplomatie zu bündeln.

Cyberdiplomatie ist ein wichtiger Teil der gesamtstaatlichen Cybersicherheit, muss aber auch die europäische oder gar die globale Dimension einbeziehen. Ermittlungen, die sich allein auf nationale Informationen stützen, reichen bei weitem nicht aus. Mit ihrem Diplomatischen Reaktionsrahmen von 2017 hat sich die EU für eine nichtmilitärische Cybersicherheitspolitik entschieden. Damit widersteht sie der Versuchung, postwendend auf Bedrohungen im Cyberraum zu reagieren. Stattdessen gibt sie politischen Maßnahmen im Rahmen der GASP den Vorrang und versucht sich so als Friedensmacht zu profilieren. Dieses deutliche politische Signal sollte von ihren Partnern und Konkurrenten in der Welt verstanden werden.

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