SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Die erneuerte Strategie der EU zur Cybersicherheit

Halbherziger Fortschritt angesichts weitreichender Herausforderungen

Annegret Bendiek/Raphael Bossong/Matthias Schulze

Im September 2017 hat die EU ihre Strategie zur Cybersicherheit aus dem Jahr 2013 aktualisiert. Damit soll Europas kritische Infrastruktur besser geschützt und die digitale Selbstbehauptung gegenüber anderen Weltregionen befördert werden. Doch die erneuerte Strategie lässt Fragen offen, wenn es darum geht, die selbstgesetzten Ziele eines »offenen, freien und sicheren Cyberraums« nach innen wie außen glaubhaft zu vertreten. Weder formuliert die EU eine klare Definition von Widerstandskraft und Abschreckung, noch wird deutlich genug, wie die institutionelle Fragmentierung und rechtliche Unverbindlichkeit in Cybersicherheitsfragen auf EU-Ebene überwunden werden sollen. Zudem bleiben kontroverse Themen ausgespart, wie die Harmonisierung des Strafrechts oder die Nutzung von Verschlüsselung. Die Mitgliedstaaten sollten ihre nationalen Alleingänge aufgeben und die gesetzliche Regulierung zur Cybersicherheit auf Ebene der Union beschleunigen.

Seit einiger Zeit ist zu beobachten, dass China sein nationales Internet immer mehr abschottet, Russland sein autoritatives Verständnis von Informationssouveränität zu verbreiten sucht und die USA eine militärisch-offensive Cyberverteidigung betreiben. Wissenschaftler sprechen bereits von der Ära des »Data Nationalism« und vom Ende des globalen Internets. Angesichts dieser strategischen Herausforderungen suchen die Mitgliedstaaten der EU einen Weg zur digitalen Selbstbehauptung. »Cyberangriffe können unter Umständen gefährlicher sein für die Stabilität von Staaten und Unternehmen als Panzer und Gewehre«, so Kommissionspräsident Jean-Claude Juncker in seiner Rede zur Lage der EU Mitte September 2017. Ende September bekräftigten die Staats- und Regierungschefs beim Digital-Gipfel in Tallinn ihre Entschlossenheit, den digitalen Binnenmarkt zu vollenden. Er soll den Flickenteppich von Regeln der 28 Mitgliedstaaten ersetzen. Im Vorfeld des Gipfels hatten sich allen voran Deutschland, Frankreich, Italien und Spanien ambitioniert gezeigt. Unter anderem hatten sie gefordert, die US-amerikanischen Internetkonzerne gemeinsam zu besteuern und für ein sicheres Umfeld zu sorgen, in dem Bürger, Unternehmen und Regierungen ihre Rechte

Dr. Annegret Bendiek ist Wissenschaftlerin, Dr. Raphael Bossong Wissenschaftler in der Forschungsgruppe EU/Europa. Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik. Dieses SWP-Aktuell wurde unter Mitarbeit von Magnus Römer, Praktikant der Forschungsgruppe EU/Europa, verfasst.

geschützt ausüben können. Digitalisierung und Cybersicherheit verlangen also mehr denn je nach verbindlichem Handeln.

Die Europäische Kommission und die Hohe Vertreterin für die Außen- und Sicherheitspolitik der EU haben daher eine breite Palette von Maßnahmen mit dem Ziel vorgeschlagen, eine »solide Cybersicherheitsstruktur« aufzubauen. Zwar bleibt die bisherige EU-Strategie für Cybersicherheit von 2013 gültig, wird aber durch ein umfangreiches Gesetzespaket aktualisiert. In der Öffentlichkeit werden einige der darin enthaltenen Vorschläge besonders lebhaft diskutiert. So soll eine Agentur der Union für Cybersicherheit geschaffen werden, mit der die Arbeit der EU-Agentur für Netz- und Informationssicherheit (ENISA) personell und finanziell verstetigt würde. Geplant ist zudem, ein europäisches System zur Zertifizierung der Cybersicherheit einzuführen, um vernetzte Geräte sowie digitale Produkte und Dienstleistungen sicherer zu machen. Darüber hinaus werden fünf Reformbereiche benannt. Erstens soll ein europäisches Forschungs- und Kompetenzzentrum für Cybersicherheit entstehen. Zweitens soll bei groß angelegten Cyberangriffen künftig ein europaweiter Krisenreaktionsmechanismus greifen. Drittens wird empfohlen, einen Cybersicherheits-Notfallfonds für den Katastrophenfall einzurichten. Viertens sollen gemeinsame Projekte in der militärischen Cyberabwehr entwickelt werden, zum einen in der Ständigen Strukturierten Zusammenarbeit, zum anderen mit Hilfe des Europäischen Verteidigungsfonds. Fünftens soll die EU auf globaler Ebene vertrauensbildende Maßnahmen und staatliche Verantwortlichkeit fördern, um Cybergefahren einzudämmen. All diese Reformvorschläge sollen dem übergeordneten Ziel dienen, die Widerstandskraft (Resilienz) der EU zu steigern.

Es wäre zu begrüßen, wenn die EU in der Cybersicherheit Europas eine bedeutendere Rolle spielte. Gewiss kann sie in diesem Bereich nicht das einzige Forum sein, vergegenwärtigt man sich die transnationale Verflechtung von technischen Infrastrukturen oder Hard- und Softwareprodukten sowie die sich wandelnden staatlichen Ambitionen im Cyberraum. Da aber der Europäische Binnenmarkt der weltgrößte gemeinsame Markt ist, bildet die EU den größtmöglichen verbindlichen Rechtsraum. In diesem Licht wirken die zahlreichen Vorschläge zur Überarbeitung der europäischen Cybersicherheitsstrategie eher halbherzig und scheinen Konfliktscheu widerzuspiegeln. Fünf Grundprobleme sollten angegangen werden. Erstens ist das Verständnis von Resilienz als strategischer Ansatz noch unzureichend. Zweitens krankt die europäische Cybersicherheit an einer institutionellen Fragmentierung und einer schwachen finanziellen Basis. Drittens fehlt es Maßnahmen zur Cybersicherheit an rechtlicher Verbindlichkeit, vor allem – viertens – bei der Harmonisierung des Strafrechts im Kampf gegen Cyberkriminalität. Fünftens schließlich bleibt unklar, wie defensive Abschreckung in der Cyberverteidigungs- und Cyberaußenpolitik auf EU-Ebene glaubwürdig funktionieren soll.

Aus diesen Gründen stellte die aktualisierte Strategie der Union keinen Wendepunkt in der immer stärker politisierten Debatte über Cybersicherheit dar. Es geht darum, dass die EU und ihre Mitgliedstaaten sich nicht auf kleinteilige Initiativen beschränken, sondern sich darüber hinaus zu Richtungsentscheidungen durchringen. Andernfalls wird die vielfach geforderte »strategische Autonomie« der EU, auch als »europäische Souveränität« verstanden, nur Rhetorik bleiben.

Resilienz als Leitbild

Wie schon in ihrer Cybersicherheitsstrategie von 2013 bevorzugt die EU in ihrem neuen Vorschlagspaket zivile, polizeiliche und militärisch-defensive Ansätze, um Systeme und Infrastrukturen der Informationstechnik (IT) zu schützen. Das damit verbundene Leitbild der Resilienz entspricht der Globalen Strategie der EU vom Juni 2016. Allerdings müssen die mit Resilienz verbundenen Konsequenzen für

europäische Cybersicherheit genauer ausbuchstabiert werden.

Der Begriff Resilienz ist kein Synonym für umfassende Sicherheit, sondern bezeichnet die Selbstregulierungskräfte eines Systems, seien sie technischer oder ökologischer Art. An die Stelle der Vermessung und Steuerbarkeit von Risiken tritt das Ideal einer dezentral verankerten und flexiblen Widerstandskraft gegen unterschiedliche wie unvorhergesehene Beeinträchtigungen. Der Ausfall einzelner Systembausteine kann dabei akzeptiert werden, weil die sogenannte schöpferische Zerstörung die Resilienz des Systems sogar stärken kann. Ein Beispiel hierfür wäre das frühe Internet, das auf radikale Selbstorganisation und dynamische Veränderungen setzte. Auf ähnliche Weise befördern viele technische Experten und Aktivisten nach wie vor die Weiterentwicklung von Open-source-Software und dezentraler Netzwerke sowie die individuelle Nutzung von Verschlüsselung.

Gleichwohl hat sich in den vergangenen Jahren auch gezeigt, dass radikal dezentrale Ansätze nicht ausreichen. Der wachsenden Verwundbarkeit von Infrastrukturen gegenüber Cyberangriffen oder Softwarefehlern kann nicht allein mit freiwilliger Kooperation und technischer Innovation begegnet werden. Cybersicherheit wird gerade in liberalen Gesellschaften zunehmend als öffentliches Gut gesehen, das nur durch verbindliche Regulierung erzeugt werden kann. Um aber einen angemessenen Ausgleich zwischen garantierter Stabilität und dezentraler Offenheit des Cyberraums zu erreichen, sollte die EU ein präziseres Verständnis von Resilienz ausarbeiten. Dazu bedarf es nachvollziehbarer Kriterien, wann und warum je nach Themenfeld der Cybersicherheit welche Instrumente zum Aufbau von Widerstandskraft greifen sollten.

Es ist sinnvoll, dass die Kommission in der aktualisierten Strategie einen gesamtgesellschaftlichen Ansatz für Resilienz fordert, der marktwirtschaftliche, gesellschaftliche und politische Akteure einbezieht. Kernstück des digitalen Binnenmarkts soll ein einheitlicher Markt für Cybersicherheit werden, der auf »eingebauter Sicherheit« (security by design) in vernetzten Geräten fußt. Pflichten zur Cyberhygiene – also der regelmäßigen Pflege und Vorsorge bei der Nutzung vernetzter Geräte und des Internets – betreffen jeden einzelnen Marktteilnehmer, da das Verhalten des schwächsten Gliedes für die Widerstandskraft des Gesamtsystems ausschlaggebend ist. So kann es zur Cyberhygiene beitragen, wenn unsichere Systeme öffentlich vorgeführt werden. Zugleich wird in der aktualisierten Strategie der Fachkräftemangel im Bereich IT und Cybersicherheit als fundamentale Herausforderung benannt. Vorschläge für harmonisierte Ausbildungsgänge sind hier zwar hilfreich, doch besitzt die EU kaum einschlägige Kompetenzen im Bildungsbereich. Auf europäischer Ebene soll es derweil gemeinsame »Blaupausen« zum Verhalten in Krisenreaktionen sowie verstärkte Cybersicherheitsübungen geben.

All diese Ansätze entsprechen der Idee einer verteilten Widerstandskraft, lassen aber keine klare Rangfolge erkennen, mit der auch strukturelle Veränderungen in den Mitgliedstaaten forciert werden könnten. Ein derart vager Begriff von europäischer Resilienz ist nicht geeignet, den gewünschten gesamtgesellschaftlichen Paradigmenwechsel anzustoßen, im Gegenteil. Er kann sogar schlecht koordinierte Vorgehensweisen, fehlende Verantwortlichkeiten oder die geringe Mobilisierung von Ressourcen kaschieren. Blaupausen, Zertifikate und Bildungspläne garantieren noch keine gelebte Krisenresistenz und operative Sicherheit. Es bedürfte detaillierterer Konzepte, wie die EU trotz geringer rechtlicher Kompetenzen gerade in der frühzeitigen Bildung voranschreiten kann. Nur so wird sich die Lücke bei den digitalen Fertigkeiten und dem entsprechenden Humankapital (digital skills gap) langfristig schließen lassen. Das gilt auch für Initiativen zum Awareness-Training, also zum Aufbau eines Bewusstseins für Bedrohungen aus dem Cyberraum. Für die weitere Diskussion wäre es notwendig, Zielvorstellungen von Resilienz zu definieren, zum Beispiel

Vertrauen zu schaffen oder Schäden und Ausfallzeiten zu minimieren. Dabei sollte stets Bezug auf unterschiedliche Bedrohungsszenarien genommen und auf dieser Basis bewertet werden, welche Ressourcen einzuplanen wären.

Institutionelle und finanzielle Fragmentierung

Eine einheitliche gesetzliche Regulierung auf EU-Ebene würde dabei helfen, das Problem der institutionellen Fragmentierung in der Cybersicherheit entschiedener anzugehen. In der aktualisierten Strategie der EU werden in diesem Kontext wichtige Bereiche identifiziert. Die ENISA soll aufgewertet werden, um die Standardisierung und die Umsetzung des Rechtsrahmens der EU für mehr Sicherheit in informationellen Infrastrukturen zu verbessern. Zu diesem Zweck ist vorgesehen, das Aufgabenspektrum der Agentur zu erweitern und ihr Budget zu erhöhen. Sie soll ihre Kooperation mit verschiedenen Akteuren vertiefen, vor allem mit dem gleichfalls zu stärkenden Cybercrime Centre (EC3) im europäischen Polizeiamt Europol. Dabei soll sie auch mehr operative Lösungen anbieten, etwa One-Stop-Shops für den Umgang mit akuten Cyberangriffen. Dies bedeutet, dass Unternehmen bei grenzüberschreitenden Datentransfers künftig nur noch einen Ansprechpartner für die Beurteilung datensicherheitsrechtlicher Belange haben, auf dessen Aussagen sie sich dann auch verlassen sollten. Daneben wird zurzeit ein weiteres Exzellenzzentrum und -netzwerk geplant. Sowohl in der Forschung als auch bei der Verbreitung neuer Sicherheitstechnik soll es eine zentrale Rolle spielen und vergleichbare nationale Zentren miteinander verbinden. Der militärische Bereich und damit die Europäische Verteidigungsagentur (EDA) soll hier schrittweise einbezogen werden. Zudem soll das neue Cyberzentrum die Zertifizierungsprozesse der ENISA »untermauern«, während die Agentur für strategische Gefahrenanalysen zuständig bleibt.

Zwar lassen sich nicht alle Aufgaben sinnvoll in einer einzigen Cybersicherheitsagentur der EU bündeln. Dennoch müssen die genannten Schnittstellen und Schwerpunkte so schnell wie möglich ausgestaltet werden. Andernfalls könnten vor allem große Mitgliedstaaten die Entwicklung eines vernetzten Vorgehens auf EU-Ebene erschweren, etwa aus Prestigegründen oder weil sie bereits Ressourcen für eigene Lösungen aufgewendet haben. So fördert die Bundesregierung den Aufbau eines Zentrums zur Cyberabwehr in München. Frankreich wiederum betreibt verstärkt eine strategische Politik zur Forschungsförderung im Bereich Künstliche Intelligenz. Bisher ist es nur ein politischer Wunsch der Kommission, dass diese Strukturen in einem europäischen Netzwerk aufgehen. Noch nicht einmal die Rolle der ENISA gegenüber nationalen Cybersicherheitsstellen ist hinreichend geklärt. Das gilt beispielsweise mit Blick auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITis).

Alle staatlichen Behörden konkurrieren mit der Privatwirtschaft um IT-Fachkräfte, sind aber häufig als Arbeitgeber weniger attraktiv. Die Institutionen der EU sollten unnötige Konkurrenz um qualifiziertes Personal vermeiden. Deshalb sollten personelle Ressourcen für die akuten Sicherheitsherausforderungen stärker gebündelt werden. Maßnahmen für Bildung und dezentralen Resilienzaufbau in sämtlichen Mitgliedstaaten können erst langfristig Wirkung entfalten.

Darüber hinaus sollten sich die Mitgliedstaaten, wie in der Strategie gefordert, umfassend an der finanziellen Unterfütterung des neuen Exzellenznetzwerks beteiligen. Das ist dringend notwendig angesichts der gewaltigen Summen, die Staaten wie China, Indien und die USA in ihre IT-Industrien und -Forschung investieren. Der von der Kommission vorgeschlagene Cybersicherheits-Notfallfonds kann nur den Anfang einer Umschichtung von Haushaltsmitteln der EU bilden. Allerdings besteht die Gefahr,

dass die Verhandlungen über den nächsten Mehrjährigen Finanzrahmen der EU in Debatten über nationale Nettobeiträge und den Ausgleich fehlender Zahlungen des Vereinigten Königreichs verhaftet bleiben, statt strategische Investitionen im IT-Bereich zu ermöglichen.

Schwache Standardsetzung

Erhöhte Resilienz gegen Cybergefahren setzt auch die Bereitschaft zur weiteren rechtlichen Harmonisierung voraus. In ihrer erneuerten Strategie betont die EU zu Recht, wie wichtig die Zertifizierung von IT-Produkten in diesem Zusammenhang ist. Dafür wäre der europäische (digitale) Binnenmarkt der geeignete Raum, in dem auch globale Standardisierungsprozesse vorangetrieben werden könnten. In der erneuerten Strategie ist vorgesehen, dass eine verschärfte Zertifizierung und Produktsicherheitsüberprüfung zwischen ENISA und privatwirtschaftlichen Akteuren immer noch auf freiwilliger Basis stattfindet. Doch die Erfahrungen bei der Genese der EU-Richtlinie zum Schutz kritischer Informationsinfrastrukturen (NIS) haben gezeigt, dass derlei Ansätze an Grenzen stoßen. Zahlreiche freiwillige Konsultationen und öffentlich-private Partnerschaften haben erwiesen, dass strukturelle Hürden bei der Meldung von Cyberangriffen und bei Vorsorgemechanismen oftmals bestehen bleiben. Diesem Missstand soll mit der NIS-Richtlinie begegnet werden. Sämtliche Betreiber und Anbieter »essentieller Dienste«, etwa in den Bereichen Energie, Wasserversorgung, Transport, Finanzwesen, Gesundheit und Internet, sind nun verpflichtet, hinreichende Investitionen und organisatorische Reformen für Cybersicherheit zu veranlassen. Zudem müssen die Mitgliedstaaten der EU gemäß Richtlinie nationale Meldesysteme schaffen.

In ihrer erneuerten Cybersicherheitsstrategie legt die EU einen Schwerpunkt auf die weitere Ausgestaltung der NIS-Richtlinie unter Leitung der ENISA. Ein Hauptproblem dabei bilden die stark voneinander abweichenden Umsetzungskapazitäten der Mitgliedstaaten. Mittelfristig wird zudem die Definition kritischer Infrastrukturen aus der NIS-Richtlinie zu diskutieren sein, denn auch Internet-Provider oder kleinere Digitalfirmen können Einfallstore für Angriffe sein.

Vor diesem Hintergrund überrascht der zurückhaltende Ansatz der erneuerten Strategie. Eine verbindliche statt einer freiwilligen Produktzertifizierung sowie eine Haftungspflicht (liability) für Soft- und Hardwarehersteller hätten hier wichtige Impulse setzen können. Traditionell zentralisierte Infrastrukturen überschneiden sich zunehmend mit der privaten Nutzung technischer Geräte im sogenannten Internet der Dinge, was vielfache neue Verwundbarkeiten schafft. Verbindliche Zertifikate und Produkthaftung könnten Hersteller aus anderen Weltregionen unter Zugzwang setzen, neue und vorausschauende europäische Regulierungen umzusetzen, wenn sie weiterhin im Binnenmarkt wirtschaften wollen. Ein frühes regulatorisches Handeln könnte europäischen Firmen Wettbewerbsvorteile verschaffen (first mover advantage). Die wachsende öffentliche Nachfrage seitens der Nutzer nach Produktsicherheit im IT-Bereich rechtfertigt es, so bald wie möglich von freiwilligen zu verpflichtenden Standardisierungsprozessen überzugehen.

Bekämpfung der Cyberkriminalität

Auch jenseits des Binnenmarkts bleiben die gesetzgeberischen Reformambitionen der EU beschränkt. Um aber Cyberkriminalität effektiv einzudämmen, ist es nötig, Straftatbestände und Möglichkeiten der strafverfolgenden Behörden zu harmonisieren. Zwar wird in der Strategie das laufende Gesetzgebungsvorhaben der Union zur erleichterten grenzüberschreitenden Übermittlung elektronischer Beweismittel angeschnitten. Auch der Vorschlag, das technische Kommunikationsprotokoll IPv6 möglichst breit zu nutzen, kann helfen, die IT-Forensik zu erleichtern. Andere wichtige Debatten zur Strafverfolgung blieben jedoch weitgehend unberücksichtigt. Dies

betrifft zunächst das gemeinschaftliche Vorgehen privater Firmen und staatlicher Stellen gegen Cyberkriminalität. Die vorgeschlagene Ausarbeitung von Leitlinien (guidelines) zu einer datenschutzrechtlich abgesicherten Zusammenarbeit kann nur ein erster Schritt sein. Schon heute wird weit intensiver darüber diskutiert, wie sich die Spannung zwischen dem neueren europäischen Datenschutzrecht und der dynamisch wachsenden privatwirtschaftlichen Datensammlung auf den Binnenmarkt auswirken wird. Seit Jahren ist am Beispiel USA zu besichtigen, dass privatwirtschaftliche Zusammenarbeit mit Strafverfolgungsbehörden im Cyberraum verbindliche Regeln benötigt, um Überwachungsskandale oder vertrauensschädigende juristische Auseinandersetzungen zu vermeiden.

Weiterhin fehlt in der erneuerten Strategie der EU eine klare Aussage dazu, ob Verschlüsselungstechnologien geschwächt werden sollten, um Strafverfolgungsbehörden den Zugriff auf Computersysteme zu erleichtern. Verschlüsselung ist jedoch ein tragender Pfeiler von Cybersicherheit durch Resilienz, etwa für den Fall, dass Hacker oder Geheimdienste sich unerlaubt fremder Daten bemächtigen wollen. Alle Mitgliedstaaten der EU werden gemeinsam entscheiden müssen, ob »Hintertüren« oder eine »Quellen-Telekommunikationsüberwachung«, also die Online-Durchsuchung von Endgeräten, zugelassen werden sollen. Dabei müssen die Mitgliedstaaten im Blick behalten, ob ihre Entscheidung im Sinne eines nachhaltigen Regimes grenzüberschreitender polizeilicher und strafrechtlicher Zusammenarbeit wäre. Verhandlungen über Verschlüsselung werden unter den europäischen Innenministern bereits geführt. Das Thema fand wohl eher aus politischen denn aus inhaltlichen Gründen keinen Eingang in die aktualisierte Strategie.

Ebenfalls ausgeklammert blieb die Kontroverse über die strafrechtliche Definition und Verfolgung von Inhalten im Internet und in sozialen Medien. Zwar haben die meisten Mitgliedstaaten der EU die Budapester Konvention unterzeichnet und sich damit verpflichtet, Delikte im Cyberraum strafrechtlich zu verfolgen. Weit auseinander gehen indes die juristischen Auffassungen darüber, welche Handlungen im digitalen Bereich als Straftaten zu bewerten sind. Strittig ist vor allem die Reichweite der Meinungsfreiheit, wie am Problem der Hassreden deutlich wird. Während die Kommission einen weiteren freiwilligen Verhaltenskodex mit der Privatwirtschaft erarbeitet hat, sind mehrere europäische Mitgliedstaaten dabei, strengere Haftungsregeln für Anbieter sozialer Medien zu verabschieden. Nationale Alleingänge sind jedoch nur begrenzt effektiv und gefährden möglicherweise die Meinungsfreiheit innerhalb wie außerhalb der EU. Autoritäre Regime wie Russland berufen sich in diesem Kontext mittlerweile ausdrücklich auf das deutsche Netzwerkdurchsetzungsgesetz vom September 2017. Probleme aufgrund nationaler Regelungen werden dadurch verschärft, dass private Akteure dazu angehalten werden, in Eigenregie Inhalte zu löschen. Häufig hatte dies zur Folge, dass Meinungsäußerungen zu stark eingeschränkt wurden. Auch im Hinblick auf global agierende Unternehmen wie Facebook oder Google ist es daher notwendig, dass die EU verbindliche gesetzliche Regeln schafft. Darin müssen ausgewogene und durchsetzbare Mechanismen zum Schutz essentieller Persönlichkeitsrechte und zum Umgang mit illegalen Inhalten definiert sein.

Cyberverteidigung und Cyberaußenpolitik

Wenig Neues enthält die überarbeitete Strategie der EU, wenn es um die Normensetzung auf globaler Ebene geht, also um Regeln für staatliches Verhalten im Cyberraum. Dies verwundert ein wenig, wird doch weltweit immer mehr über digitale Souveränität und Cyberabschreckung diskutiert. In der Cyberverteidigung verfolgt die EU weiterhin einen defensiven Ansatz. Dies steht im Einklang mit dem Leitbild der Resilienz, dem gemäß bestimmte Risiken in

Kauf zu nehmen und deren Auswirkungen zu mindern sind. Darauf aufbauend könnte allerdings präziser gefasst werden, wie sich systemische Widerstandskraft mit einer effektiven Abschreckung vertragen soll. Resilienz schreckt in erster Linie planmäßig herbeigeführte Ausfälle von Internetdiensten (denial of service) ab oder auch strategische Cyberoperationen, mit denen kritische Infrastrukturen funktionsunfähig gemacht werden sollen. Desinformationskampagnen aus dem Ausland oder Cyberkriminelle werden hingegen eher durch aktivere Maßnahmen und effektive Strafverfolgung abgeschreckt. Ein Ansatzpunkt wären daher weitere bilaterale Abkommen zur Cyberkriminalitätsbekämpfung zwischen der EU und Drittstaaten.

Für Zwecke der Cyberverteidigung wiederum verweist die EU vor allem auf die bestehende Zusammenarbeit mit der Nato, die mögliche Rolle der Ständigen Strukturierten Zusammenarbeit der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) sowie das finanzielle Potential des im Juni 2017 beschlossenen Verteidigungsfonds. Aufgrund unterschiedlicher Fähigkeiten und digitaler Transformationsprozesse in den nationalen Streitkräften ergibt es zwar Sinn, die Cyberkooperation in der GSVP zu flexibilisieren. Auch ist es zweckmäßig, dass die EU den Akzent auf gemeinsame Übungen und die Entwicklung von Kapazitäten in schwächeren Mitgliedstaaten legt. Gleichwohl stellt sich die Frage, wie diese Länder Anschluss finden und den neuen Verteidigungsfonds nutzen sollen, wenn sie sich wegen schwacher Strukturen gerade nicht an der Ständigen Strukturierten Zusammenarbeit im Cyberbereich beteiligen können. Derweil bleibt die Nato der erste sicherheitspolitische Bezugspunkt für Europas Cyberverteidigung. So hatte der Europäische Rat bereits im Dezember 2013 beschlossen, die Zusammenarbeit zwischen EU und Nato zu intensivieren, und im November 2014 ein Rahmenkonzept zur Cyberverteidigung (Cyber Defence Policy Framework) verabschiedet. Damit sollen die Missionen im Rahmen der GSVP besser geschützt und die Kommunikationssicherheit des Europäischen Auswärtigen Dienstes (EAD) erhöht werden. Die Zusammenarbeit zwischen EU und Nato bei der Abwehr hybrider Gefahren und damit auch von Cyberangriffen soll über die Anfang April 2017 eingerichtete Hybrid Fusion Cell in Helsinki stattfinden. Hier sind Nato- und EU-Staaten im Aufsichtsrat vertreten. Trotz Übungen mit Beteiligung beider Partner jedoch bleibt der gemeinsame strategische Rahmen unklar. Im Tallinn Manual von 2013 und 2017 hat das Nato-Zentrum für die Abwehr von Cyberangriffen Vorschläge unterbreitet, das Recht zum Krieg (ius ad bellum) und das Recht im Krieg (ius in bello) für den Cyberraum zu kodifizieren. Dies kann aber nicht als gemeinsame Linie der EU und ihrer Mitgliedstaaten betrachtet werden.

Auch die wissenschaftliche Forschung sieht digitale Gegenschläge, wie sie die Nato erwägt, kritisch. Oft können weder die Urheber von Cyberattacken noch Ziele für Gegenschläge bestimmt werden (was als Attributionsproblem bezeichnet wird). Die Gefahr ist groß, unbeteiligte oder gekaperte Systeme zu attackieren, die womöglich kritische Versorgungsaufgaben in anderen Ländern erfüllen. Zudem steht zu befürchten, dass eine Eskalationsspirale gegenseitiger Cyberangriffe in Gang gesetzt wird. Dieses Problem ist besonders dringlich, da einige Firmen bereits digitale Gegenangriffe (hack-backs) praktizieren. Gemäß dem EU-Leitbild der Resilienz müssten von staatlicher Seite sowohl rote Linien als auch die Stufen der Eskalationsbereitschaft einschließlich entsprechender Sanktionen definiert werden. Dies setzt die Schaffung einheitlicher Attributionsstandards und ein gemeinsames Lagebewusstsein (situational awareness) für Cyberbedrohungen voraus. Dazu böten sich die ENISA oder das Zentrum zur Abwehr hybrider Bedrohungen in Helsinki an. Unstrittig ist auch, dass weitere politische Mittel vonnöten sind, um Konfliktspiralen im Cyberraum zu vermeiden. Die EU will hierzu einen Sanktionskatalog ausarbeiten, die sogenannte Cyber Diplomacy

Toolbox, um mögliche Gegenmaßnahmen im Falle eines Cyberangriffs von außen festzulegen. Der Katalog umfasst politische, wirtschaftliche und strafrechtliche Sanktionen, die Einbestellung von Diplomaten und auch digitale Antworten. All dies hat zum Ziel, die Kosten des Angreifers für seine Cyberattacken zu erhöhen. Allerdings sind auch diplomatische Reaktionen vom Grundproblem der Attribution betroffen. Und da der Einsatz der Toolbox freiwillig ist und zudem einstimmige Unterstützung durch die EU-Mitgliedstaaten erfordert, stehen einer kohärenten und effizienten defensiven Abschreckung zahlreiche Hindernisse entgegen.

Schließlich hat die EU in ihrer modifizierten Strategie erklärt, sie wolle Fragen der Cybersicherheit in relevanten Außenbeziehungen eine gewisse Priorität einräumen. Als Ansatzpunkt wird eine weitere »Plattform« vorgeschlagen, um Drittstaaten in ihren Cybersicherheitskapazitäten zu unterstützen. Dies ist in erster Linie als Zugeständnis an osteuropäische Staaten zu werten, um die Nachbarschaft der Union besser vor Einflussnahme aus Russland zu schützen. Weitere globale Verhandlungsprozesse und Normensetzungen für Cybersicherheit werden hingegen nur noch am Rande erwähnt.

Ausblick: Digitalmacht EU

Die Reformvorschläge der erneuerten EU-Strategie zur Cybersicherheit vom September 2017 sind ein Schritt in die richtige Richtung, um die Union technisch, rechtlich und strategisch besser gegen Cyberangriffe zu wappnen. Widerstandskraft lässt sich aber nur dann aufbauen, wenn die Mitgliedstaaten strategische Weichenstellungen vornehmen und die Schwachstellen konsequent angehen. Ambitionierte Vorschläge treffen dabei vielfach auf Widerstand. So betrachten einige Mitgliedstaaten nicht die EU, sondern die OECD als angemessenen politischen Rahmen für Fragen der IT-Regulierung. Vertreter der Industrie im Bereich Informations- und Kommunikationstechnologien (IKT) beklagen, den Institutionen der EU fehle es am notwendigen Sachverstand.

Gerade deshalb muss die EU ihre Zurückhaltung aufgeben, die in der erneuerten Cybersicherheitsstrategie zu erkennen ist. Der erste Lackmustest wird der Europäische Zertifizierungs- und Kennzeichnungsrahmen für IKT-Sicherheit sein. Um zügig eine verbindliche Regulierung von IT-Produkten anzugehen, sollte unter Leitung von ENISA und Europäischer Kommission möglichst schnell Einigkeit über hinreichende Sicherheitsstandards zwischen allen Mitgliedstaaten hergestellt werden. Privatwirtschaft und Wissenschaft sind an diesem Prozess zu beteiligen. Einer Verständigung förderlich dürfte die Einsicht sein, dass die europäische Industrie auf Wettbewerbsgleichheit im Weltmarkt angewiesen ist.

Die größte Herausforderung für einen vielschichtigen Resilienzaufbau in der Cybersicherheit liegt aber nach wie vor darin, für belastbare und vertrauensvolle Beziehungen zwischen allen Beteiligten zu sorgen. Das gilt für das Verhältnis starker und schwächerer Cybernationen in der IKT untereinander ebenso wie für jenes zwischen Mitgliedstaaten, EU-Behörden und privaten Akteuren. Immer wichtiger in diesem Zusammenhang werden klare strategische Leitlinien der EU für die Cyberaußenpolitik und damit verbundene Entscheidungen. Dazu zählt, die Verschlüsselung zu stärken oder auf Cyberbedrohungen aus dem außereuropäischen Raum mit politischen, wirtschaftlichen und strafrechtlichen Sanktionen zu antworten.

Auf sich gestellt sind die Mitgliedstaaten und die Unternehmen für diese Aufgaben und Verhandlungen zu schwach. Andererseits ist Vorsicht geboten, sollte die EU sich anschicken, allzu weitreichende Regulierungen ins Auge zu fassen. Will sie aber zur Digitalmacht werden, sind in allen genannten Bereichen enge Kooperation, ein verbindlicher europäischer Rechtsrahmen und technische Standardisierung unabdingbar.

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