Digitale Agenda und Cybersicherheit

Annegret Bendiek

Im grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehr spielen digitale Informationssysteme, allen voran das Internet, eine wesentliche Rolle. Die fortschreitende Vernetzung macht es notwendig, gemeinsame datenschutzrechtliche und sicherheitspolitische Regelungen zu treffen. Die digitale Integration ist analog zur wirtschaftlichen Integration als der Ausbau einheitlicher gesellschaftlicher Handlungsräume zu verstehen, die gemeinsamen Regeln unterliegen und durch die Aufhebung von institutionellen Grenzen zwischen den Mitgliedstaaten gekennzeichnet sind. Die Europäische Kommission schätzt, dass die Vollendung des digitalen Binnenmarkts das europäische Bruttoinlandsprodukt um fast 500 Mrd. Euro steigern könnte. Estland hatte in der zweiten Jahreshälfte 2017 die EU-Ratspräsidentschaft inne und gilt als Vorreiter der Digitalisierung in Europa. Die nationale „e-ID"-Infrastruktur wird von nahezu allen Bürgern genutzt. Das Land hat weltweit acht Duplikate der eigenen digitalen Staatsverwaltung aufgebaut, die von den estnischen Botschaften betreut werden. Die IT-Infrastruktur dieser „Daten-Botschaften" wird mit Hilfe von privaten Unternehmen in befreundeten Staaten wie Großbritannien, Deutschland, den USA, Kanada, Südafrika und Japan betrieben. Man erhofft sich davon unter anderem, dass der digitale Binnenmarkt vollendet und die Rechtsverbindlichkeit zur Cybersicherheit erhöht wird. All dies weist in die richtige Richtung, da Europa mit der Gemeinsamen Außen- und Sicherheitspolitik (GASP)[1], dem Europäischen Auswärtigen Dienst (EAD) und der Hohen Vertreterin für Außen- und Sicherheitspolitik als diejenige Ebene benannt wird, auf der mitgliedstaatliche Sicherheit und Verteidigung ausgebaut werden sollen. „Cyberangriffe können unter Umständen gefährlicher sein für die Stabilität von Staaten und Unternehmen als Panzer und Gewehre",[2] so Kommissionspräsident Jean-Claude Juncker in seiner Rede zur Lage der Union 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 geschützt ausüben können. Digitalisierung und Cybersicherheit verlangen also mehr denn je nach verbindlichem Handeln.[3]

1 Siehe auch den Beitrag „Gemeinsame Außen- und Sicherheitspolitik" in diesem Buch.

2 Europäische Kommission: Juncker-Rede zur Lage der Union 2017: Den Wind in unseren Segeln nutzen, 13. September 2017, abrufbar unter: https://ec.europa.eu/germany/news/20170913-juncker-rede-zur-lage-der-union-2017_de (letzter Zugriff: 21.11.2017).

3 European Commission: Digital Agenda Review: Frequently Asked Questions, 18. December 2012, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-12-1000_en.htm (letzter Zugriff: 16.6.2017).

Herausforderungen des digitalen Binnenmarkts

Die Herausforderungen bei der Schaffung eines digitalen Binnenmarkts umfassen die Soft- und Hardware-Branche, das Kommunikationsnetz, den Bereich des Cloud Computing, effektive und umfassende Datenschutzrichtlinien sowie die Quasi-Monopolstellungen großer digitaler Unternehmen.

Europa ist in der Soft- und Hardware-Branche heute mit wenigen Ausnahmen wie SAP oder Alcatel-Lucent kaum noch ein relevanter Spieler. Durch den Rückgang des Marktanteils europäischer Anbieter (Siemens, Nokia) besteht de facto eine Duopolstellung zwischen US-amerikanischen und asiatischen Anbietern (Huawei, ZTE). Dieser Duopolstellung muss mit angemessenen, EU-weiten Regulierungen begegnet werden.

Des Weiteren ist ein verlässliches europäisches Kommunikationsnetz, das im allgemeinen öffentlichen Interesse betrieben und verwaltet wird, für den weiteren Ausbau des digitalen Binnenmarkts sehr wichtig. Leider ist in Europa zur Zeit genau das Gegenteil der Fall, da sich das europaweite Netz aus nationalen Teilnetzen mit Kontrolleuren, die jeweils partikulare Interessen verfolgen, zusammensetzt. Dadurch ist der Schutz persönlicher Daten, beispielsweise vor Zugriffen des Bundesnachrichtendienstes, nicht gewährleistet.

Außerdem steht die Europäische Union im Bereich des Cloud Computing vor vielfältigen Herausforderungen, da im Bereich des europäischen Konsumenten- und Datenschutzes das Problem des Auseinanderfallens von rechtlichen und ökonomischen Räumen besteht. Die Digitalisierung der Kommunikation hat außerdem dazu geführt, dass das Recht auf Privatheit nicht mehr in dem nötigen Umfang gewährleistet ist. Verschiedenste Formen von Cyberattacken, von Phishing-Mails, über „Denial of Service"-Attacken zu klassischen Viren und Trojanern, bedrohen zunehmend private Kommunikation, öffentliche Diskurse und kritische Infrastrukturen. Es bedarf einer europäischen Antwort auf die Gefährdung privater Daten, demokratischer Meinungsbildung und lebenswichtiger Einrichtungen und Infrastruktur. Die Quasi-Monopolstellungen großer Unternehmen führen bekanntermaßen zu Missbrauch, höheren Preisen und schlechteren Produkten. Es gibt zwar Fusionskontrollen, jedoch reagiert das europäische Wettbewerbsrecht erst dann mit Sanktionen, wenn Marktbeherrschung auch faktisch zu Missbrauch führt. Beispielsweise hatte der ehemalige Wettbewerbskommissar Joaquín Almunia bereits 2010 ein Verfahren gegen Google eingeleitet, das von seiner Nachfolgerin Margrethe Vestager wiederbelebt wurde: Unter anderem schränke der Konzern die Möglichkeiten von Unternehmen ein, auf ihren Webseiten Suchmaschinenwerbung von Googles Wettbewerbern anzuzeigen. Im Juni 2017 verhängte die Kommission aufgrund von Überbevorteilung der Google-eigenen Onlinehandel-Angebote Strafzahlungsforderungen von 2,42 Mrd. Euro gegen den Konzern. Ferner wird das weltweit dominierende Smartphone-Betriebssystem Android untersucht. Grundsätzlich kann die Kommission Strafzahlungen in der Höhe von bis zu zehn Prozent des Jahresumsatzes eines Konzerns fordern. Zudem geht die Wettbewerbskommissarin gegen mehrere Staaten vor, weil diese möglicherweise Konzerne wie Amazon oder Apple durch Steuervorentscheide („tax rulings") bevorzugen. Diese sind zumindest dann wettbewerbswidrig, wenn einzelne Unternehmen auf Kosten ihrer Konkurrenten bevorzugt werden.[4]

4 Siehe auch den Beitrag „Wettbewerbspolitik" in diesem Buch

Die digitale Gesamtstrategie[5] – Datenschutz und Datensicherheit als Standortvorteil

Anfang Juni 2015 hat die Kommission ihre Gesamtstrategie zur Schaffung eines digitalen Binnenmarkts in der Europäischen Union[6] vorgestellt. Sie beruht auf drei Säulen: 1) besserer Zugang für Verbraucher und Unternehmen zu digitalen Waren und Dienstleistungen in ganz Europa, 2) Schaffung der richtigen Bedingungen und gleichen Voraussetzungen für florierende digitale Netze und innovative Dienste und 3) bestmögliche Ausschöpfung des Wachstumspotenzials der digitalen Wirtschaft. Die jüngsten Gesetzesinitiativen beziehen sich auf den grenzüberschreitenden E-Commerce und eine Reform der Richtlinie über audiovisuelle Mediendienste mit neuen Vorgaben vor allem für Video-Plattformen im Internet. Im Juli 2016 verkündete die Kommission zudem eine öffentlich-private Partnerschaft mit der European Cyber Security Organisation (ECSO) und im Januar 2017 einigte sie sich auf einen Reformentwurf zur Regulierung der Privatsphäre für elektronische Kommunikation (ePrivacy), welcher nun vom Rat verhandelt wird.

Der Schutz vertraulicher Daten, die aufgrund mangelnder Sicherheitsvorkehrungen oder nachteiliger rechtlicher Rahmenbedingungen in die Hände Dritter gelangen können, gilt als Hauptaugenmerk der EU-Regulierungen. Im Dezember 2015 haben sich das Europäische Parlament, der Rat und die Kommission auf eine neue Datenschutz-Grundverordnung (DS-GVO) geeinigt. Damit wird 2018 die seit 1995 erste umfassende Reform des EU-Datenschutzrechts in Kraft treten. Mit der DS-GVO wird es erstmals ein einheitliches und verbindliches Schutzniveau für die gesamte Union geben. An die neuen Regeln müssen sich nicht nur europäische Unternehmen halten, sondern auch die aus Drittstaaten wie den USA. Die neue DS-GVO soll zudem Garantierechte für EU-Bürger bei der Rechtsbeihilfe durchsetzen und wird Auswirkungen auf alle derzeit zu verhandelnden bilateralen Abkommen mit den USA zum Datentransfer im Sicherheits- und Wirtschaftsbereich haben.

Wie schon in ihrer Cybersicherheitsstrategie von 2013 bevorzugt die Europäische Union 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 vom Juni 2016. Allerdings müssen die mit Resilienz verbundenen Konsequenzen für europäische Cybersicherheit genauer ausbuchstabiert werden. Eine verschärfte Zertifizierung und Produktsicherheitsüberprüfung zwischen der EU-Agentur für Netz- und Informationssicherheit ENISA und privatwirtschaftlichen Akteuren findet noch auf freiwilliger Basis statt. Die Genese der EU-Richtlinie zum Schutz kritischer Informationsinfrastrukturen (NIS) hat 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 bestehen bleiben. Diesem Missstand soll mit der verbesserten Implementierung 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 gemäß Richtlinie nationale Meldesysteme schaffen. Ein Hauptproblem

5 Siehe ausführlich Annegret Bendiek: Digitale Agenda und Cybersicherheit, in:Weidenfeld, Werner/Wolfgang Wessels (Hrsg.): Jahrbuch der Europäischen Integration 2016, Baden-Baden 2016, S. 229-240.

6 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und sozialausschuss und den Ausschuss der Regionen. Strategie für einen digitalen Binnenmarkt für Europa, KOM(2015) 192 final.

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.

Cybersicherheit als Querschnittsaufgabe

Institutionell wird Cybersicherheit auf Ratsarbeitsebene als Querschnittsaufgabe gefasst und in der Horizontal Working Party on Cyber Issues bearbeitet. Tritt ein großer Cybervorfall ein, soll fortan eine ganze Reihe von EU-Einrichtungen miteinander kooperieren.[7] Wie die noch gültige Cybersicherheitsstrategie soll auch die künftige Strategie Politikfelder übergreifend angelegt sein. Die bisherige Strategie enthält fünf Handlungsfelder: Resilienzaufbau, Bekämpfung von Cyberkriminalität, Aufbau einer Cyberverteidigung, Entwicklung der industriellen und technischen Ressourcen sowie schließlich Erarbeitung einer globalen Strategie für den Cyberraum. Während aber die europäische Zusammenarbeit bei der Cyberkriminalitätsbekämpfung bereits erfolgreiche Ermittlungen durch Europol verbuchen konnte, bleibt es in der Cyber-Außen- und Verteidigungspolitik bis dato bei gut gemeinten Absichtserklärungen.[8]

Spätestens der Angriff vom Mai 2017 auf mehr als 200.000 Computersysteme in über 150 Ländern hat jedoch die Augen dafür geöffnet, dass die scharfe Trennung zwischen innerer und äußerer Sicherheit beim Schutz kritischer Infrastruktur problematisch ist. Verteidigungsunion und Sicherheitsunion sind zwar formal klar voneinander getrennt, diese formale Trennung wird in der Cybersicherheitspolitik aber durchbrochen. Sie bildet eine Schnittstelle zwischen der inneren und äußeren Sicherheit sowie von Innen-, Außen- und Verteidigungspolitik im europäischen Mehrebenensystem. Damit ist sie zugleich ein Brennpunkt für die neuen Herausforderungen, die mit dem Ausbau der Sicherheits- und Verteidigungsunion einhergehen.

Die Sicherheitsunion findet ihren Ursprung im Konzept „Raum der Freiheit, der Sicherheit und des Rechts“. Umgesetzt wird es durch die Programme von Tampere (1999-2004), Den Haag (2005-2009) und Stockholm (2010-2015). Vertraglich verankert ist es im Vertrag von Lissabon (Art. 3 Abs. 2 EUV). Das aktuelle Kommissionsprogramm sowie die Umstrukturierung der Kommission gehen ein Stück weiter. Von Beginn an hatten sie eine stärkere Vernetzung innerer und äußerer Sicherheit sowie von Innen- und Außenpolitiken zum Ziel. Nach den Anschlägen auf die französische Satirezeitschrift Charlie Hebdo stellte die Kommission im April 2015 die Europäische Sicherheitsagenda[9] vor. Laut Kommissionspräsident Jean-Claude Juncker sind organisierte Kriminalität, Terrorismus und Cyberkriminalität grenzüberschreitende Herausforderungen, die „eine gemeinsame europäische Aufgabe“ darstellen und eine vertiefte europäische Zusammenarbeit im Rahmen einer Europäischen Sicherheitsagenda begründen. Ein Jahr später kündigte die Kommission als Reaktion auf die Terroranschläge in Brüssel vom März 2016 an, eine Sicherheitsunion aufzubauen. Rechtlich soll diese im Wesentlichen auf Art. 67 AEUV unter Berücksichtigung von Art. 4 Abs. 2 EUV und Art. 72 AEUV beruhen. Demnach schafft die Union „einen Raum der Freiheit, der Sicherheit und des Rechts“, auch als Schengen-Raum bekannt. Mit der Umsetzung der „Schengensicherheit“ wurde ein im September 2016 neu

7 Hierzu zählen European Network and Information Security Agency (ENISA), CERT-EU, EC3, die EU-Justizbehörde Eurojust, die EU-Hybrid Fusion Cell, INTCEN sowie die EAD.

8 Siehe auch den Beitrag „Gemeinsame Außen- und Sicherheitspolitik“ in diesem Buch.

9 Europäische Kommission: Eine Europäische Sicherheitsagenda, COM(2015) 185 final.

ernannter Kommissar, Julian King, betraut. Als seine wichtigsten Aktionsfelder nannte er a) die Verbesserung des rechtlichen Rahmens in der Terrorismusbekämpfung, b) Prävention und Deradikalisierung, c) einen verbesserten Informationsaustausch zwischen den mitgliedstaatlichen Behörden, d) den Aufbau von Datenbanken und deren Interoperabilität, e) den Grenzschutz und f) besseren Schutz kritischer Infrastrukturen. Bislang wurden sieben Fortschrittsberichte zur Umsetzung vorgelegt. Unter anderem wurde inzwischen ein Terrorabwehrzentrum im Europäischen Polizeiamt (Europol) geschaffen, das Waffenrecht verschärft, eine Antiterrorismusrichtlinie und eine Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) erlassen. Für eigene Auswertungs- und Ermittlungstätigkeiten greifen die Polizeibehörden in Europa immer häufiger auf Daten aus unterschiedlichen Quellen zurück. Deshalb müssen sie sich mit riesigen Datenbeständen beschäftigen und mit ihnen forensisch grenzüberschreitend umgehen. Europol wird künftig eine immer wichtigere Rolle bei der Übermittlung personenbezogener Daten spielen. Bisher hat das Polizeiamt mit den USA, Kanada, Norwegen, der Schweiz und Australien Vereinbarungen über operative Kooperation getroffen. Auf staatlicher und EU-Ebene wird kein Weg an einem gebündelten Management der Informationstechnologie vorbeiführen.

Cyberverteidigung

Neben engerer Verzahnung von Planung und Führung nationaler Streitkräfte steht vor allem eine Harmonisierung der Akquise im Fokus. Ende November 2016 unterbreitete die Kommission Pläne für einen Europäischen Verteidigungsfonds,[10] der gemeinsame Investitionen in Forschung und Entwicklung fördern soll.[11] Zum einen soll gemeinsame Forschung zu Verteidigungstechnologien gefördert werden, etwa zu Elektronik, Metawerkstoffen, verschlüsselter Software oder Robotertechnik. Dazu hat die Kommission 25 Mio. Euro für 2017 eingeplant. Sie vermutet, dass dieser Betrag bis 2020 auf 90 Mio. Euro pro Jahr steigen könnte. Im mehrjährigen Finanzrahmen der Europäischen Union nach 2020 soll ein Verteidigungsforschungsprogramm in Höhe von rund 500 Mio. Euro pro Jahr enthalten sein. Zum anderen soll die gemeinsame Rüstungsbeschaffung erleichtert werden, etwa bei verschlüsselter Software, womit jährlich um die 5 Mrd. Euro eingespart werden sollen. Zu diesem Zweck will die Kommission die Europäischen Struktur- und Investitionsfonds (ESI-Fonds) sowie die Europäische Investitionsbank (EIB)[12] unterstützen, die Entwicklung von Gütern und Technologien mit doppeltem Verwendungszweck („dual use“) zu finanzieren. Ferner sollen die allgemeinen Richtlinien zur Vergabe öffentlicher Aufträge auf den Verteidigungs- und Sicherheitsbereich ausgedehnt werden. Auf diese Weise soll grenzüberschreitende Zusammenarbeit gefördert und die Entwicklung gemeinsamer Industrienormen vorangetrieben werden. Cybersicherheit fußt nicht nur auf mehr Vernetzung innerer und äußerer Sicherheit in der Europäischen Union, sondern ist auch ein wesentliches Betätigungsfeld innerhalb der NATO. Gemäß eines Rahmenabkommens vom März 2003 (Berlin Plus) darf die Europäische Union bei militärischen Operationen auf Mittel und Fähigkeiten der NATO zurückgreifen. Auch die gemeinsamen Erklärungen der beiden Organisationen von Juli und Dezember 2016 spiegeln die Leitidee der globalen Strategie wider, dass sich das Gebiet der Union nur durch Zusammenarbeit wirkungsvoll verteidigen lasse. Es wurden 42 Maßnahmen beschlossen, um in sieben Aktionsfeldern die

10 Siehe auch den Beitrag „Gemeinsame Sicherheits- und Verteidigungspolitik“ in diesem Buch.
11 Siehe auch den Beitrag „Forschungs-, Technologie- und Telekommunikationspolitik“ in diesem Buch.
12 Siehe auch den Beitrag „Europäische Investitionsbank“ in diesem Buch.

auf dem Warschauer Gipfel vom Juli 2016 vereinbarte intensivierte Zusammenarbeit zu beschleunigen. Hierzu zählen die Abwehr hybrider Bedrohungen, Frühwarnung und Lagebild, parallele Operationen in identischen Gebieten, Cybersicherheit und -abwehr, interoperable Fähigkeiten, Verteidigungsindustrie und Forschung sowie Übungen, um die Resilienz von EU- und NATO-Partnern zu stärken. Die meisten Mitgliedstaaten befürworten hierbei eine enge Koordination von NATO- und EU-Streitkräften. Alle Maßnahmen in der Außen-, Sicherheits- und Verteidigungspolitik sollen demnach automatisch auch die NATO stärken oder zumindest deren Aufgabenspektrum ergänzen. Ein Beispiel hierfür ist die Einrichtung der EU-Hybrid Fusion Cell im Europäischen Auswärtigen Dienst (EAD). Sie soll Informationen aus den Sicherheitsbehörden der NATO- und EU-Staaten, aus EU-Institutionen sowie den Partnerstaaten bündeln. Auf dieser Basis soll sie für die Frühwarnung sorgen und das Lagebild zur Abwehr hybrider Bedrohungen wie Cyberangriffen erstellen. Für die Zusammenarbeit mit der NATO spricht zudem, dass die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) allein nach außen gerichtet, eine Territorialverteidigung nicht vorgesehen und ein Einsatz im Innern der Union vertraglich ausgeschlossen ist. Gleichwohl bildet die Landesverteidigung eine Kernaufgabe für die NATO als Verteidigungsbündnis. Die derzeit laufende Überarbeitung der Europäischen Cybersicherheitsstrategie wird all diese Initiativen in der inneren und äußeren Sicherheit ebenso berücksichtigen müssen wie die Entwicklungen bei der Datensicherheit im digitalen Binnenmarkt.

Mit dem EU-Cyber Defence Policy Framework vom November 2014 hält die Europäische Union ihre Mitgliedstaaten dazu an, ihre Cyberverteidigungsfähigkeiten für die GSVP und die Einhaltung ihrer Bündnisverpflichtungen zu überprüfen. Auch verlangt der EU-Militärstab besseren Schutz gegen Cyberangriffe auf EU-Operationen und -Missionen. Die seit 2015 intensivierte EU-NATO-Zusammenarbeit[13] in der Cybersicherheit und -verteidigung wurde mit der Warschauer Erklärung im Juli 2016 formalisiert und auf dem gemeinsamen Treffen der Außenminister der EU- und NATO-Staaten im Dezember 2016 mit konkreten Umsetzungsvorschlägen untermauert. Im November 2016 machte sich das Europäische Parlament ausdrücklich dafür stark, die Kooperation in der Cyberverteidigung zu vertiefen. Dazu forderte es die Mitgliedstaaten auf, gemeinsam mit der European Defence Agency (EDA) und dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) die dafür notwendigen Fähigkeiten auszubauen. Die EDA soll hierbei Synergien zwischen den Fähigkeitsentwicklungen von NATO und Europäischer Union schaffen. Projekte zur Cyberverteidigung sind unter anderem die Collaboration Database (CoDaBa) und der Capability Development Plan (CDP). Zu den Projekten der EU-NATO-Kooperation Frühwarnfähigkeiten für Hauptquartiere und Systeme zur Gefahrenerkennung (MASFAD). Die Überarbeitung der Europäischen Cybersicherheitsstrategie hat all diese Initiativen in der inneren und äußeren Sicherheit ebenso berücksichtigen müssen wie die Entwicklungen bei der Datensicherheit im digitalen Binnenmarkt.

Die Europäische Kommission und die Hohe Vertreterin für die Außen- und Sicherheitspolitik 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,

13 Siehe auch den Beitrag „Die Europäische Union und die NATO“ in diesem Buch.

mit der die Arbeit der 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 Union auf globaler Ebene vertrauensbildende Maßnahmen und staatliche Verantwortlichkeit fördern, um Cybergefahren einzudämmen. All diese Reformvorschläge sollen dem übergeordneten Ziel dienen, die Widerstandskraft (Resilienz) der Europäischen Union zu steigern.

Es wäre zu begrüßen, wenn die Union 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.

Ausblick

Die Europapolitik wird nicht umhinkommen, sich mit Grundsatzfragen zur außen- und sicherheitspolitischen Weichenstellung der Europäischen Union zu befassen.

(1) Eine Vertiefung der GSVP ist durchaus ambivalent zu betrachten. Entwickeln sich die Sicherheits- und die Verteidigungsunion tatsächlich zu neuen Kernelementen des Integrationsprozesses, kann dies eine normative Gewichtsverlagerung der Union bedeuten: weg vom kosmopolitischen Anspruch der Marktintegration und hin zu einem protektionistischen Integrationsprojekt. Es sollte vermieden werden, dass mit einem Europa der Sicherheit und Verteidigung alte Konfrontationsmuster, Sicherheitsdilemmata und ein Rüstungswettlauf zurückkehren, gerade in der Cybersicherheit. Der notwendige Prozess der Formulierung eines europäischen Weißbuchs zur Sicherheit und Verteidigung sollte daher insbesondere zwei defensive Elemente betonen, bei denen vertrauens- und sicherheitsbildende Maßnahmen im Mittelpunkt stehen.

(2) Die Europäische Union und ihre Mitgliedstaaten müssen sich einig werden, was einen „digitalen Verteidigungsfall" auslöst. Hierzu gehört eine gemeinsame Antwort auf die Frage, ob ein Angriff auf kritische Infrastrukturen auch ein „offensives Verteidigen", also eine sofortige militärische Reaktion, erlauben soll. Attacken auf kritische Infrastrukturen und die systematische Nutzung von Sicherheitslücken privater Akteure stellen die Politik zusätzlich vor das Problem, wie Abwehrmaßnahmen auf einzelstaatlicher und EU-Ebene gleichzeitig koordiniert werden und welche Rollen Diplomatie und Militär dabei spielen sollen.

(3) Die Europäische Union benötigt dringend Verantwortung für den Aufbau von Resilienz in der Netzwerk- und Informationssicherheit, und zwar in der Rechtsform einer Verordnung. Bislang ist die ENISA formal dafür zuständig, in Notfällen die Fähigkeit zur schnellen Reaktion seitens der Mitgliedstaaten und deren reibungslose EU-weite Zusammenarbeit zu gewährleisten. Noch immer werden allerdings viel zu viele kritische Infrastrukturen ausschließlich auf nationaler oder privater Ebene gesichert. Der Austausch von Informationen über Cyberrisiken ist nicht nur zwischen der Europäischen Union und den

Mitgliedstaaten mangelhaft, sondern auch zwischen den europäischen Agenturen Europol, Eurojust, EDA und ENISA. Die zuständigen Generaldirektionen arbeiten nur eingeschränkt zusammen und erhalten häufig von den Mitgliedstaaten nicht die nötigen Informationen, um ein europaweites Sicherheitsnetz knüpfen zu können. Für die Reform der Cybersicherheitsstrategie der Europäischen Union gilt auch, die Rolle des EAD und die zivilen Instrumente der Cyberdiplomatie, also vertrauens- und sicherheitsbildende Maßnahmen, ebenso weiterzuentwickeln wie die Cyber Diplomacy Toolbox von 2016 und 2017. Anhand dieses Sanktionskatalogs kann die Europäische Union politische, finanzielle und rechtliche Maßnahmen ergreifen, um auf jene Cyberangriffe zu reagieren, die rechtlich unterhalb der Schwelle eines bewaffneten Konflikts liegen.

Weiterführende Literatur

Annegret Bendiek: Das Neue Europa der Sicherheit. Elemente für ein europäisches Weißbuch für Sicherheit und Verteidgung, in: SWP-Aktuell, Juni 2017.

Annegret Bendiek: Die Globale Strategie für die Außen- und Sicherheitspolitik der EU, in: SWP-Aktuell 44, Juli 2016.

Annegret Bendiek/Evita Schmieg: EU-Außenhandel und Datenschutz. Wie lässt sich beides besser vereinabren?, in: SWP-Aktuell 10, Februar 2016.

Jerin Lanier: Wenn Träume erwachsen werden. Ein Blick auf das digitale Zeitalter, Essays und Interviews 1984-2015, Hoffmann und Campe 2015.