SSOAR

Open Access Repository

www.ssoar.info

Das neue "Europa der Sicherheit": Elemente für ein europäisches Weißbuch zur Sicherheit und Verteidigung

Bendiek, Annegret

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Bendiek, A. (2017). *Das neue "Europa der Sicherheit": Elemente für ein europäisches Weißbuch zur Sicherheit und Verteidigung.* (SWP-Aktuell, 37/2017). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-55075-3

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

SWP Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Das neue »Europa der Sicherheit«

Elemente für ein europäisches Weißbuch zur Sicherheit und Verteidigung

Annegret Bendiek

Im Juli 2017 übernimmt Estland den Vorsitz im Rat der EU. Estlands Hauptthemen werden die Digitalisierung sowie Europas gemeinsame Außen-, Sicherheits- und Verteidigungspolitik sein. Damit greift die Ratspräsidentschaft wichtige Herausforderungen für Europa auf. Gleichzeitig kann sie ein weit geöffnetes Gelegenheitsfenster nutzen, denn die Regierungen der EU-Mitgliedstaaten betrachten eine Vertiefung europäischer Außen- und Sicherheitspolitik heute wohlwollender als jemals zuvor. Auch der Kommission ist das Thema Sicherheit seit Beginn ihrer Amtszeit ein ständiges Anliegen – von Kommissionspräsident Junckers Politischen Leitlinien vom Juli 2014 bis zu seiner vorerst letzten Rede zur Lage der Union im September 2016. Politik und Gesellschaft unterstützen ein »Europa der Sicherheit«, das auf drei Großprojekten aktueller Europapolitik aufbaut: einer Sicherheitsunion, einer Verteidigungsunion und einer engen Zusammenarbeit zwischen Nato und EU. Beim Schutz kritischer Infrastrukturen, also in der Cybersicherheit, verschmelzen diese Projekte. Alle drei sollten in einem übergreifenden Weißbuch mit einer gemeinsamen strategischen Ausrichtung versehen werden.

Gewaltsame Konflikte und Umbrüche in der östlichen und südlichen Nachbarschaft der EU, neue hybride Bedrohungen und terroristische Anschläge haben die Bereitschaft in Politik und Gesellschaft verstärkt, die Zusammenarbeit in der europäischen Außen-, Sicherheits- und Verteidigungspolitik zu intensivieren. Auch die Erklärung von Rom, die der Europäische Rat im März 2017 abgab, macht deutlich, dass die Sicherheit der Bürger und des Gebiets der EU von der Politik und einer gesellschaftlichen Mehrheit als neues Integrationsnarrativ getragen wird. Das bedeutet auch, dass die EU in einem Europa der Sicherheit ihre neue Bestimmung finden will. Federica Mogherini, Hohe Vertreterin der EU für Außen- und Sicherheitspolitik, sowie Jyrki Katainen, Vizepräsident der Europäischen Kommission und zuständig für Beschäftigung, Wachstum, Investitionen und Wettbewerbsfähigkeit, unterstützen eine sicherheitspolitische Vertiefung. Im Januar 2017 plädierten sie dafür, die EU zu einer echten Verteidigungsunion auszubauen, die nicht auf die EU-27 begrenzt ist. Die Sicherheit der Union könne nur durch Maßnahmen im Außenbereich und eine enge Zusammenarbeit mit der Nato verbessert werden. Das neue »Europa der Sicherheit« beruht auf

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

drei Großprojekten aktueller Europapolitik: einer Sicherheitsunion, einer Verteidigungsunion und einer intensiven Kooperation zwischen EU und Nato. Alle drei sind in der europäischen Cybersicherheit miteinander verbunden und finden hier einen wichtigen gemeinsamen Bezugspunkt. Spätestens der Angriff vom Mai 2017 auf mehr als 200 000 Computersysteme in über 150 Ländern hat die Augen dafür geöffnet, dass die scharfe Trennung zwischen innerer und äußerer Sicherheit beim Schutz kritischer Infrastruktur problematisch ist. Aus der wahrgenommenen Notwendigkeit, ein »Europa der Sicherheit« zu konzipieren, erklärt sich der politische Aktionismus in allen Bereichen der Sicherheits- und Verteidigungspolitik, wie sich in der aktuellen Umsetzung der Globalen Strategie der EU (EUGS) seit Juli 2016 zeigt.

Umsetzung der Globalen Strategie

Der bevorstehende Austritt Großbritanniens aus der EU sowie die Unberechenbarkeit in Donald Trumps Amtsführung als Präsident der USA sind Hauptmotive für die EU, das in der EUGS vom Juli 2016 zwar genannte, aber nicht definierte Ziel der »strategischen Autonomie« ernsthaft anzugehen. Aus Sicht Trumps und seiner Regierung tun die meisten Staaten Europas zu wenig für dessen Sicherheit. Angesichts der mageren Bilanz europäischer Transformationsbemühungen in ihren Nachbarländern versucht die EU nun, ihren Bürgern mit Hilfe der EUGS den Mehrwert der Union in Sicherheitsfragen zu verdeutlichen. Um die Sicherheit der Bürger und des Territoriums der EU zu gewährleisten, wurden im November 2016 folgende Prioritäten formuliert: a) auf Krisen und Konflikte in den Grenzregionen der EU zu reagieren, b) Fähigkeiten in Nachbarregionen aufzubauen und c) die EU und ihre Staatsbürger zu schützen. Die Union soll verstärkte Widerstandskraft (Resilienz) entwickeln, also die Fähigkeit, besser auf Terroranschläge, Veränderungen im Cyberraum und hybride Bedrohungen zu reagieren. Um diesen Anspruch einzulösen, soll der sogenannte umfassende Ansatz, das heißt die kohärente Nutzung militärischer, ziviler und wirtschaftlicher Instrumente, ebenso dienen wie die stärkere Vernetzung innerer und äußerer Sicherheit. Die Staaten des Weimarer Dreiecks schlugen sogar im August 2016 vor, ein eigenständiges Format des Europäischen Rats zu schaffen, das sich ausschließlich mit Fragen innerer und äußerer Sicherheit beschäftigt. Die deutsche Verteidigungsministerin sprach sich im November 2016 für das Fernziel einer Europäischen Sicherheits- *und* Verteidigungsunion aus. Verteidigungsunion und Sicherheitsunion sind aber formal klar voneinander getrennt. Beim Projekt Sicherheitsunion handelt es sich um eine maßgeblich von der Kommission vorangetriebene Initiative, die sich in erster Linie auf Fragen der Innen- und Justizpolitik bezieht. Die Verteidigungsunion dagegen ist ein politisches Projekt von Außen- und Verteidigungsministern. Diese formale Trennung wird in der Cybersicherheitspolitik durchbrochen. Sie bildet eine Schnittstelle zwischen den Großprojekten 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.

Politische Initiativen

Die Idee einer Sicherheits- und Verteidigungsunion ist nicht neu, betraf früher aber hauptsächlich die äußere Dimension von Sicherheit. Schon 2002 verkündeten im Prozess des damaligen Europäischen Konvents die Außenminister Deutschlands und Frankreichs, Joschka Fischer und Dominique de Villepin, die ESVP solle zu einer Sicherheits- und Verteidigungsunion fortentwickelt werden. Seit Sommer 2016 plädieren Deutschland und Frankreich nicht nur für engere Zusammenarbeit in der Verteidigungspolitik, sondern auch in der inneren Sicherheit. Beide Staaten setzen sich für ein »Europa der verschiedenen

Geschwindigkeiten« ein. Dabei wollen sie mehr als bisher auf Verfahren der flexiblen Integration wie der verstärkten Zusammenarbeit (Art. 20 Abs. 1 EUV), der ständigen strukturierten Zusammenarbeit (Art. 42 Abs. 6 und Art. 46 EUV) sowie auf konstruktive Enthaltungen (Art. 31 EUV) zurückgreifen. Europäische Sicherheit ist nämlich schon jetzt funktional und regional variabel organisiert. Weder an der Politik zur inneren Sicherheit noch an der Verteidigungspolitik sind alle Mitgliedstaaten formal beteiligt. In der Innen- und Justizpolitik machen Großbritannien, Irland und Dänemark Gebrauch von der Opt-out-Klausel. Dänemark nimmt zudem nicht an den gemeinsamen Entscheidungsverfahren der GSVP teil. Auch sind nicht alle Mitgliedstaaten der EU in der Nato. Das trifft auf Finnland, Irland, Malta, Schweden, Zypern und Österreich zu.

Sicherheitsunion

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 vor. Laut Kommissionspräsident 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 EU »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 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 wurde verschärft und es wurden 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.

Verteidigungsunion

In seinem Bericht vom Oktober 2016 über die künftige militärische Zusammenarbeit der EU forderte das Europäische Parlament, eine neu geschaffene Verteidigungsunion solle die engere Verzahnung der nationalen

Truppen ermöglichen und die seit 2007 existierenden, aber noch nie eingesetzten Battlegroups in stehende Einheiten umwandeln. Zudem sollen die Mitgliedstaaten intensiver bei der Beschaffung von Rüstungsgütern zusammenarbeiten, die derzeit noch zu ungefähr 80 Prozent über rein nationale Märkte stattfinde. Der Kommission zufolge verursacht diese Praxis jährliche Kosten von bis zu 100 Milliarden Euro. Während seiner Ansprache zur Lage der Union im September 2016 ermahnte Kommissionspräsident Juncker die Mitgliedstaaten, ihre Verteidigungsanstrengungen stärker miteinander zu koordinieren. Ende November 2016 legte die Kommission den Europäischen Verteidigungs-Aktionsplan (EDAP) vor. Die darin formulierten Ziele gehen weit über die 2008 beschlossenen zivil-militärischen Headline Goals hinaus. Auch heißt es dort, dass dafür Sorge getragen werden soll, gleichzeitig zehn zivile und fünf militärische Operationen führen zu können. Eine europäische militärische Planungs- und Führungsfähigkeit (MPCC) soll bis Juni 2017 aufgebaut sein. Die bisher überwiegend politischen Erklärungen der Mitgliedstaaten sollen rechtsverbindlicher werden.

Ende November 2016 unterbreitete die Kommission Pläne für einen Europäischen Verteidigungsfonds, der gemeinsame Investitionen in Forschung und Entwicklung fördern soll. Zum einen soll gemeinsame Forschung zu Verteidigungstechnologien gefördert werden, etwa zu Elektronik, Metawerkstoffen, verschlüsselter Software oder Robotertechnik. Dazu hat die Kommission 25 Millionen Euro für 2017 eingeplant. Sie vermutet, dass dieser Betrag bis 2020 auf 90 Millionen Euro pro Jahr steigen könnte. Im mehrjährigen Finanzrahmen der EU nach 2020 soll ein Verteidigungsforschungsprogramm in Höhe von rund 500 Millionen Euro pro Jahr enthalten sein. Zum anderen soll gemeinsame Rüstungsbeschaffung erleichtert werden, etwa bei verschlüsselter Software oder Hubschraubern. Damit sollen um die 5 Milliarden Euro jährlich eingespart werden. Zu diesem Zweck will die Kommission die Europäischen Struktur- und Investitionsfonds sowie die Europäische Investitionsbank (EIB) 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 befördert und die Entwicklung gemeinsamer Industrienormen vorangetrieben werden.

Aspekte des »dual use« geraten immer mehr in den Blick. Eine Reihe aktueller Projekte der Europäischen Verteidigungsagentur (EDA) befasst sich mit der Frage, wie Forschungsergebnisse gleichermaßen für innere und äußere Sicherheit verwandt werden können. Die ersten beiden Forschungsaufträge wurden zu unbemannten Luftfahrtsystemen und zu mobilen Aufklärungsrobotern für die urbane Kriegsführung vergeben. Ein drittes Konsortium erhielt den Auftrag, eine autonome Überwachungsplattform sowohl für äußere als auch innere Sicherheit zu entwickeln. Autonome Aufklärungssysteme, zum Beispiel Drohnen und Sensoren, sollen mit Lasern und Störsendern zu einem Schwarm verbunden (EuroSWARM) und unter ein zentrales Kommando gestellt werden können. Einsatzmöglichkeiten sieht die EDA vor allem in Grenzkontrolle und Überwachungssicherheit.

EU-Nato-Zusammenarbeit

Europäische Sicherheit fußt nicht nur auf mehr Vernetzung innerer und äußerer Sicherheit in der EU, sondern ist auch ein wesentliches Betätigungsfeld innerhalb der Nato. Gemäß einem Rahmenabkommen vom März 2003 (Berlin Plus) darf die EU 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 zwischen EU und Nato wirkungsvoll verteidigen lasse.

Es wurden 42 Maßnahmen beschlossen, um in sieben Aktionsfeldern die 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 GSVP allein nach außen gerichtet, eine Territorialverteidigung nicht vorgesehen und ein Einsatz im Innern der EU vertraglich ausgeschlossen ist. Gleichwohl bildet die Landesverteidigung eine Kernaufgabe für die Nato als Verteidigungsbündnis.

Brennpunkt Cybersicherheit

Cyberangriffe auf Staaten und kritische Infrastrukturen sind schon lange Realität. Quantität und Qualität solcher Attacken wachsen stetig. Selbst die Grenze zwischen offensiver und defensiver Ausrichtung ist fließend. Hat ein Akteur die Fähigkeit zur Verteidigung, kann er auch weltweit angreifen. Die Schwierigkeit der Attribution, also der Fähigkeit, einen Angriff zweifelsfrei einem Verursacher zuzuordnen, ist Ausdruck der faktischen politischen, technischen und rechtlichen Grenzenlosigkeit des Cyberraums. Der Cyber- und Informationsraum kennt weder nationale Grenzen noch ein institutionelles Gefüge. Cybersicherheitspolitik ist ein zwischen Mitgliedstaaten und EU-Ebene geteilter Kompetenzbereich. Im Juli 2016 trat die Richtlinie »über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union« (NIS-Richtlinie) in Kraft. Damit wurde ein einheitlicher europäischer Rechtsrahmen geschaffen, um EU-weit nationale Kapazitäten für die Cybersicherheit bereitzustellen, mehr Zusammenarbeit der EU-Staaten zu ermöglichen sowie Mindestsicherheitsanforderungen an und Meldepflichten für bestimmte Dienste des Schutzes kritischer Infrastruktur zu formulieren. Um einheitliche Maßnahmen in diesem Sinne vorzubereiten, werden derzeit zwei neue Koordinierungsmechanismen aufgebaut. Eine Kooperationsgruppe soll die strategische Zusammenarbeit und den Informationsaustausch über Cybervorfälle zwischen den Mitgliedstaaten unterstützen, während das Netz der IT-Noteinsatzteams (CSIRT) für die Nothilfe vor Ort zuständig ist.

Querschnittsaufgabe

Cybersicherheitspolitik in der EU beruht nicht nur auf der NIS-Richtlinie, sondern auch auf der Cybersicherheitsstrategie von 2013 sowie der Strategie für einen digitalen Binnenmarkt von 2015. Außerdem baut sie auf den jüngsten Mitteilungen über die Umsetzung der Europäischen Sicherheitsagenda von 2015 und zur Abwehr hybrider Bedrohungen von 2016 auf. Institutionell wird Cybersicherheit auf Ratsarbeitsebene als Querschnittsaufgabe gefasst und in der Horizontal Working Party on Cyber Issues bearbeitet. Cybersicherheit liegt auch im Krisenfall an der Schnittstelle ziviler und militärischer Zusammenarbeit sowie innerer und äußerer Sicherheit. Tritt ein großer Cybervorfall ein, soll fortan eine ganze Reihe von EU-Einrichtungen miteinander kooperieren. Hierzu zählen die Europäische

Agentur für Netz- und Informationssicherheit (ENISA), das IT-Notfallteam der EU (CERT-EU), das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die EU-Justizbehörde Eurojust, die EU Hybrid Fusion Cell, das Zentrum für Informationsgewinnung und -analyse (INTCEN) im EAD sowie die EDA. Wie die noch gültige Cybersicherheitsstrategie soll auch die künftige Strategie politikfeldübergreifend 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.

Cyberverteidigung

Mit dem EU Cyber Defence Policy Framework vom November 2014 hält die 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-geführte Operationen und Missionen. Die seit 2015 intensivierte Zusammenarbeit zwischen EU und Nato 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 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 EU schaffen. Projekte zur Cyberverteidigung sind unter anderem die Collaboration Database (CoDaBa) und der Capability Development Plan (CDP). Zu den Projekten der Kooperation zwischen EU und Nato gehören Frühwarnfähigkeiten für Hauptquartiere und Systeme zur Gefahrenerkennung (MASFAD).

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. Die Erwartungen an die kommende estnische Ratspräsidentschaft sind hoch. Man erhofft sich davon unter anderem, dass der digitale Binnenmarkt vollendet und die Rechtsverbindlichkeit zur Cybersicherheit erhöht wird. Estland gilt als digitaler Vorreiter im Binnenmarkt und will gleichzeitig die europäische Cyber-Außen- und Verteidigungspolitik in enger Kooperation mit der Nato weiterentwickeln. All dies weist in die richtige Richtung, da Europa mit der GASP, dem EAD und der Hohen Vertreterin für Außen- und Sicherheitspolitik als diejenige Ebene benannt wird, auf der mitgliedstaatliche Sicherheit und Verteidigung ausgebaut werden sollen.

Elemente für ein Weißbuch

Für die estnische Ratspräsidentschaft 2017 wird es vor allem darauf ankommen, welchen Mehrwert sie Europa in Fragen der Digitalisierung und der GASP/GSVP verschaffen kann. In die Zeit der Ratspräsidentschaft Estlands fällt auch die Endphase des Reflexionsprozesses über das Weißbuch der Kommission zur Zukunft der EU. Die Ratspräsidentschaft wird nicht umhinkommen, sich mit Grundsatzfragen zur außen- und sicherheitspolitischen Weichenstellung der EU zu befassen, die, wie einige Politiker fordern, Eingang in ein »Europäisches Weißbuch zur Sicherheit und Verteidigung«

finden sollten. Denn das angepeilte »Europa der Sicherheit« 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 von vier Hauptelementen getragen sein, bei denen vertrauens- und sicherheitsbildende Maßnahmen im Mittelpunkt stehen.

1. Das Streben nach »strategischer Autonomie« der EU ist ein hoher und auf den ersten Blick reizvoller Anspruch. Er steht allerdings im Widerspruch zur Idee einer zusammenwachsenden und interdependenten Welt, in der Konflikte nicht einseitig (»strategisch autonom«), sondern durch Dialog und Kooperation beigelegt werden. Daher muss geklärt werden, was der Begriff für das Verhältnis zwischen EU und Nato bedeutet. Grundsätzlich konkurriert die Vorstellung strategischer Autonomie mit dem Ziel, den europäischen und den amerikanischen Pfeiler westlicher Sicherheitspolitik fester zu verbinden. Deshalb gilt es allen Forderungen aus Wissenschaft und Politik entgegenzutreten, die USA mögen sich aus Europa zurückziehen oder Europa solle einen eigenen Nuklearschirm schaffen. Stattdessen sollte der Nexus zwischen dem nordamerikanischen und dem europäischen Pfeiler der Nato verstärkt werden. Zudem wäre über weitere gemeinsame Rüstungsprojekte nachzudenken. Nicht strategische Autonomie, sondern strategische Verflechtung sollte das Ziel sein.

2. Wollen EU und Nato künftig noch intensiver zusammenarbeiten, müssen beide Seiten sich darüber 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 europäischer Ebene gleichzeitig koordiniert werden und welche Rollen Diplomatie und Militär dabei spielen sollen. In ihrem Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr warnt die Bundesregierung, Terrororganisationen nutzten »soziale Medien und digitale Kommunikationswege, um Ressourcen zu generieren, Anhänger zu gewinnen, ihre Propaganda zu verbreiten und Anschläge zu planen«. Mehr und mehr seien sie in der Lage, mit Cyber-Fähigkeiten Ziele anzugreifen oder Chemikalien für Attentate zu verwenden. Sogar der Einsatz biologischer und radioaktiver Substanzen sei künftig nicht völlig auszuschließen.

Wie würde ein betroffener Staat in der EU darauf reagieren? Welche Formen des Handelns würde die Beistandsverpflichtung umfassen? Cyberangriffe sind meist nicht eindeutig einem Verursacher zuzuordnen. Dies erschwert eine rechtliche Bewertung, inwiefern es angezeigt ist, politische, rechtliche, nachrichtendienstliche, polizeiliche und/oder militärische Mittel einzusetzen. Im Falle einer Katastrophe oder eines Anschlags gestatten die Solidaritätsklausel (Art. 222 AEUV) und die Beistandsklausel (Art. 42 Abs. 7 EUV) unmittelbare Hilfe durch die Mitgliedstaaten. Die Solidaritätsklausel gewährleistet, dass alle Beteiligten auf nationaler und EU-Ebene zusammenarbeiten, um schnell, effektiv und einheitlich auf einen Terroranschlag, eine Naturkatastrophe oder eine von Menschen verursachte Katastrophe zu reagieren. Die Beistandsklausel enthält eine Beistandspflicht der anderen Mitgliedstaaten, sollte ein Mitgliedstaat sich einem bewaffneten Angriff auf sein Hoheitsgebiet ausgesetzt

sehen. Außer zur Landesverteidigung ist aber jeglicher Einsatz deutscher Soldaten verboten, es sei denn, er ist ausdrücklich vom Grundgesetz gedeckt. Sowohl die Sicherheitsbehörden selbst als auch die für ihre Arbeit grundlegenden Gesetze wie das Trennungsgebot oder die Möglichkeiten eines Einsatzes der Bundeswehr im Innern müssen hierbei zumindest kritisch überprüft werden.

3. Die EU 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 nationale kritische Infrastrukturen ausschließlich auf nationaler oder privater Ebene gesichert. Der Austausch von Informationen über Cyberrisiken ist nicht nur zwischen der EU 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 EU 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. Anhand dieses Sanktionskatalogs kann die EU politische, finanzielle und rechtliche Maßnahmen ergreifen, um auf jene Cyberangriffe zu reagieren, die rechtlich unterhalb der Schwelle eines bewaffneten Konflikts liegen. Während der letzten Jahre sind durchaus Fortschritte bei der Cybersicherheit erzielt worden. Dies betrifft die technische Attribution, völkerrechtliche Fragen wie auch vertrauensbildende Maßnahmen in der Group of Governmental Experts (GGE) der Vereinten Nationen, in der OSZE und bei den G20.

4. Vertrauen ist eine knappe Ressource in den internationalen Beziehungen. Um mehr Vertrauen in Informations- und Kommunikationstechnologien zu schaffen, sind zusätzliche Investitionen in Technologie, Forschung, Entwicklung und Innovationsfähigkeit nötig. Im August 2016 hat die EU 450 Millionen Euro für das Forschungs- und Innovationsprogramm Horizont 2020 und damit für die Sicherheitsforschung bereitgestellt. Die Akteure des Cybersicherheitsmarkts, die von der Europäischen Cybersicherheitsorganisation (ECSO) vertreten werden, sollen ihrerseits bis 2020 die dreifache Summe investieren. Wenn es zutrifft, dass »Digitalisierung [...] die Kommerzialisierung von Forschungsergebnissen durch Wirtschaftsunternehmen« ist, wie es im August 2016 in der Frankfurter Allgemeinen Zeitung hieß, gerät die Förderung unabhängiger ziviler Sicherheitsforschung schnell unter die Räder. Nichtregierungsorganisationen wie beispielsweise das Digital Forensic Research Lab oder Big Brother Watch leisten wichtige zivilgesellschaftliche Aufklärungsarbeit. Kritische Sicherheitsforschung bildet eine notwendige Bedingung dafür, dass gesellschaftliche und demokratische Akzeptanz eines »Europas der Sicherheit« hergestellt und aufrechterhalten werden kann. Die nationalen Parlamente und das Europäische Parlament sollten dafür Sorge tragen, dass die Überwindung der Krise Europas und der Aufbau von Sicherheitsunion und Verteidigungsunion nicht auf Kosten liberaler Werte gehen. Nach wie vor wird eine große Herausforderung darin bestehen, den Vorrang der Diplomatie vor der Sicherheits- und Militärpolitik zu gewährleisten und sich allen übermäßigen Versicherheitlichungen entgegenzustellen.

© Stiftung Wissenschaft und Politik, 2017
Alle Rechte vorbehalten

Das Aktuell gibt die Auffassung der Autorin wieder

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