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

Annegret Bendiek

Sorgfaltsverantwortung im Cyberraum

Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik

S 3
März 2016
Berlin

Alle Rechte vorbehalten.
Abdruck oder vergleichbare Verwendung von Arbeiten der Stiftung Wissenschaft und Politik ist auch in Auszügen nur mit vorheriger schriftlicher Genehmigung gestattet.

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben die Auffassung der Autoren und Autorinnen wieder.

© Stiftung Wissenschaft und Politik, Berlin, 2016

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 1611-6372

Inhalt

5 **Problemstellung und Empfehlungen**

7 **Sorgfaltsverantwortung als Leitidee**

11 **Sorgfaltsverantwortung in der institutionellen Praxis**
11 Institutionelle Strukturen
15 Digitale Industriepolitik und die Bedeutung privater Akteure

19 **Cyberpolitiken im Zeichen der Sorgfaltsverantwortung**
19 Menschenrechte und Datenschutz
23 Internet Governance
24 Cyberkriminalitätsbekämpfung
27 Cyberverteidigung
29 Internationale Normenentwicklung

32 **Sorgfaltsverantwortung (noch besser) implementieren**

34 **Abkürzungsverzeichnis**

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

Diese Studie ist aus dem Projekt »Die Herausforderung der Digitalisierung für die deutsche Außen- und Sicherheitspolitik« hervorgegangen, das aus Mitteln des Planungsstabes des Auswärtigen Amtes unterstützt wurde.

Sorgfaltsverantwortung im Cyberraum Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik

Der globale Cyberraum ist in fundamentalem Wandel begriffen. Von einer »Fragmentierung des Internets« ist inzwischen häufig die Rede, doch in vielen europäischen und internationalen Arbeitsgruppen wächst das Bewusstsein dafür, dass »ein freies, offenes und gleichzeitig sicheres Internet« ein globales öffentliches Gut ist. Um dieses zu schaffen und zu bewahren, bedarf es global konzertierten Handelns auf Basis einer gemeinsamen Norm, die wechselseitige Verantwortung für einen sorgfältigen Umgang mit einzelstaatlichen Regelsetzungsprozessen verlangt. Dies entspricht der noch gültigen deutschen Cybersicherheitsstrategie von 2011 sowie der EU-Cybersicherheitsstrategie von 2013, die zivile, polizeiliche und militärisch-defensive Ansätze vorsehen, um Systeme und Infrastrukturen der Informationstechnik (IT) zu schützen.

Allerdings plädieren auch immer mehr politische Stimmen für eine Renationalisierung politischer Regelsetzung und digitale Souveränität. Die Politik muss sich der Realität stellen, dass der Cyberraum vermehrt zum Operationsfeld des Militärs wird. Das wird auch im neuen Weißbuch der Bundesregierung sowie der künftigen Cyberverteidigung von Nato und EU zum Ausdruck kommen, also in den sicherheitspolitischen Leitlinien Deutschlands und Europas sowie im Verteidigungsauftrag und in der Rüstungsbeschaffungspolitik.

Deutsche und europäische Politik sollte sich ressortübergreifend stärker an der Norm der »Sorgfaltsverantwortung« im Cyberraum orientieren, um ihr international mehr Geltung zu verschaffen. Sorgfaltsverantwortung baut auf der internationalen Rechtsnorm von Due-Diligence-Pflichten auf. Das bedeutet, alles Notwendige dafür zu tun, dass von eigenem Territorium aus keine Rechte von Dritten beeinträchtigt werden. In der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) etwa stößt Due Diligence auf weitgehende Zustimmung und bietet sich als normative Basis einer globalen Cyberordnung an. Die politische Regelsetzung der Cyber-Außen- und Sicherheitspolitik wird den technologischen Entwicklungen immer hinterherhinken. Umso wichtiger ist es, dass diese einer übergeordneten Norm unterworfen werden. Daraus ergeben sich drei unabdingbare Anforderungen an die Politik:

- Europäische Zusammenarbeit: Einbindung nationaler Politiken in den europäischen Rahmen,
- Inklusivität: breite, offen zugängliche Repräsentation unterschiedlicher Interessengruppen in der Politikformulierung,
- Zivilität: Vorrang der zivilen gegenüber der militärischen Komponente.

Europäische Zusammenarbeit: Sorgfaltsverantwortung verlangt, dass Staaten sich nicht nur untereinander, sondern auch bei der innerstaatlichen Regulierung verantwortungsvoll verhalten. Das sieht schon die Cybersicherheitsstrategie der EU von 2013 vor. In der Umsetzung der Richtlinie für Netzwerk- und Informationssicherheit (NIS) müssen alle EU-Staaten Mindeststandards und Meldepflichten in der IT-Sicherheit einführen; Betreiber kritischer Infrastruktur müssen bei der Cyberkriminalitätsbekämpfung mitwirken. Beim Aufbau des digitalen Binnenmarkts sind nationale Regelungen in Privatrecht (Datenschutz), Wirtschaftsrecht (Internet Governance) und Wettbewerbsrecht (Binnenmarkt) so zu fassen, dass zwischenstaatlichen Verantwortungspflichten Genüge getan wird. Um diesen Prozess zu beschleunigen, empfiehlt es sich, die angekündigte globale EU-Strategie für den Cyberraum rasch zu verabschieden. Nato- und EU-Staaten sind sich weitgehend einig, dass Staaten für ihr Verhalten im Cyberraum verantwortlich sind. Bei all diesen Fragen gibt es eine enge Absprache unter den »Großen Drei« Europas sowie mit der Gruppe westlicher Gleichgesinnter. Für die kommende fünfte Runde der Verhandlungen in der Gruppe der Regierungsexperten (Group of Governmental Experts, GGE) auf Ebene der Vereinten Nationen (VN) spricht vieles dafür, dass die darin vertretenen europäischen und westlichen Staaten mittelfristig die Cyberkriminalitätsbekämpfung stark machen, indem sie ihr materielles Strafrecht anpassen und zur Abschreckung nutzen. Minimalbedingungen für die globale Cybersicherheit sind die Anerkennung der Budapester Konvention zur Cyberkriminalitätsbekämpfung sowie kontinuierliche vertrauens- und sicherheitsbildende Maßnahmen (VSBM).

Inklusivität: Beim VN-Gipfel im Dezember 2015, Bestandteil des WSIS-Folgeprozesses (World Summit on the Information Society), stellte sich heraus, dass eine kurzfristige globale Einigung auf eine verbindliche Interpretation der Sorgfaltsverantwortung unwahrscheinlich ist. Daher bietet die im Dezember 2015 beschlossene Fortsetzung des Internet Governance Forum, also die Weiterverfolgung des Multistakeholder-Ansatzes, weiterhin noch am ehesten die Gewähr, dass die Idee eines weltweit freien und offenen Internets nicht den zunehmenden Sicherheitserwägungen von Regierungen zum Opfer fällt. In der Internet Governance kommt es deshalb wesentlich darauf an, einen inklusiv verstandenen Multistakeholder-Ansatz zu verstetigen und das intergouvernementale Prinzip zurückzuweisen. Die Erfahrung mit dem WSIS-Prozess der letzten zehn Jahre hat die Grenzen einer intergouvernementalen Entscheidungsfindung sichtbar gemacht. Zudem wäre es wichtig, die Norm der Sorgfaltsverantwortung für alle Stakeholder verbindlich zu machen, also für die privaten Nutzer, die Zugangsnetzbetreiber und die Transportnetz- und Internetknotenbetreiber. Langfristig sollten schiedsgerichtliche Institutionen darüber wachen, dass die Sorgfaltsverantwortung hinreichend beachtet wird.

Zivilität: Initiativen wie eine nationale Strategie zum Wirtschaftsschutz setzen auf defensive Cyberabwehr. Die Strategische Leitlinie der Bundesregierung deutet aber darauf hin, dass diese zusätzliche Verteidigungskapazitäten zur Reaktion auf Cyberangriffe aufbauen will. Von einer Entwicklung hin zur offensiven Cyberverteidigung wäre jedoch abzuraten. Nicht nur stünde sie in offenem Kontrast zur Idee der Sorgfaltsverantwortung der Cyberdiplomatie. Weil Cyberangriffe nur schlecht eindeutig zuzuordnen sind und Vergeltungsangriffe schwerwiegende unbeabsichtigte Schäden verursachen können, besteht überdies die Gefahr der Konfliktverschärfung und der Proliferation von Cyberwaffen. Die Attacke auf den Bundestag im Juni 2015 hat vor Augen geführt, wie wichtig es ist, unbeirrt auf den Aufbau resilienter Strukturen zu setzen. Die Erklärung von Souveränitätsverletzungen, der Rückgriff auf die Bündnissolidarität der Nato sowie die Cyber-Kriegserklärung der USA an den »Islamischen Staat« können nur als letzte Mittel der Politik verstanden werden. Um eine resilienzbasierte Strategie abzustützen, sind zusätzliche Mittel nötig: für die Hochsicherheitstechnologie, für die Entwicklung digitaler Forensik und für umfangreiche Maßnahmen zur Schärfung des Problembewusstseins (Awareness) in der Fortbildung des öffentlichen Dienstes, der Wirtschaft sowie in Bildung und Forschung. Zu intensivieren sind vertrauensbildende Maßnahmen in der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und der GGE. Nur auf dieser Basis ist es realistisch, bilaterale Abstimmungen wie zuletzt zwischen den USA und China zur Cyberkriminalitätsbekämpfung zu erzielen, um die Kooperation bei Aufklärung und Verfolgung grenzüberschreitender digitaler Straftaten zu verbessern und rechtsfreie Räume zu beseitigen.

Sorgfaltsverantwortung als Leitidee

> »Die Außen- und Sicherheitspolitik eines Staates kann nur in dem Maße erfolgreich sein, in dem es gelingt, mit ›einer Stimme zu sprechen‹ und das, was man ›nationale Interessen‹ nennt, klar zu kommunizieren und konsequent zu vertreten. Das heißt, dass einmal getroffene Entscheidungen innerhalb der Exekutive in gleicher Weise verstanden und umgesetzt werden müssen. Es heißt aber auch, dass überhaupt Entscheidungen getroffen werden und dass sich Stellen der Regierung verantwortlich fühlen, ein bestimmtes Problem anzugehen. Wo keine klaren Zuständigkeiten herrschen, werden Probleme oft weitergereicht und es findet eine Art ›Verantwortungsdiffusion‹ statt. Die Folge ist, dass Probleme nicht oder zu spät erkannt werden und hohe – finanzielle und politische – Kosten entstehen.«[1]

Die europäische und die deutsche Cyberdiplomatie zielen darauf ab, ein »offenes, freies und sicheres, globales Internet als Raum der Meinungsvielfalt, Teilhabe, Innovation und als Motor für Wirtschaftswachstum und Arbeit [zu] schützen und weiter aus[zu]bauen«.[2] Dieses Ziel lässt sich auch als globales öffentliches Gut beschreiben, zu dessen Bereitstellung die Kooperation aller wichtigen Staaten, Unternehmen, Wissenschaftsvertreter und der Zivilgesellschaft nötig ist.[3] Regionale Fragmentierung, Gefährdungen durch Kriminalität und eine Militarisierung des Cyberraums[4] werden nur dann zu verhindern sein, wenn die Staatengemeinschaft einschließlich aller Stakeholder im Internet[5] sich auf gemeinsame Verhaltensmaßstäbe einigt und Regelungen akzeptiert, die diese Maßstäbe verbindlich machen. Cybersicherheit ist demnach »der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind«.[6]

Die Bundesregierung, die Mitgliedstaaten der EU und die Union selbst folgen prinzipiell der Idee von »Due Diligence«[7] bei der Umsetzung ihrer Cybersicherheitsstrategien.[8] Diese Norm verpflichtet Staaten, in Friedenszeiten dafür zu sorgen, dass von ihrem Territo-

1 Christopher Daase, *Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik*, Vortrag beim CyberLab der Stiftung Wissenschaft und Politik (SWP), Berlin, 8.9.2015.

2 Die Bundesregierung, *Europäische und internationale Dimension der Digitalen Agenda*, <www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/7_Dimension/dimension_node.html> (Zugriff am 30.11.2015).

3 Wesentliche Anregungen für diese Pilotstudie beruhen auf Arbeitsgruppenergebnissen zweier Veranstaltungen, den SWP-CyberLabs mit rund 60 Teilnehmern in den Räumen der Stiftung Wissenschaft und Politik in Berlin (8.9.2015) und der Ständigen Vertretung der Bundesrepublik Deutschland bei der Europäischen Union in Brüssel (18.11.2015). Besonderer Dank gilt Prof. Dr. Christopher Daase (Goethe-Universität, Frankfurt/Main) sowie Prof. Scott Shackelford (Indiana University, Bloomington, USA) und allen Teilnehmern der Exekutive und Legislative und anderen Stakeholdern für ihre konstruktive Mitarbeit.

4 In der Cybersicherheitsstrategie der Bundesregierung heißt es: »Der Cyber-Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. IT-Systeme in einem isolierten virtuellen Raum sind kein Teil des Cyber-Raums.« Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland*, Berlin 2011, S. 14, <www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>.

5 »Das Internet ist ein weltweiter Verbund öffentlich erreichbarer Netze. Die Netze werden unabhängig voneinander betrieben, nutzen aber einen gemeinsamen Adressraum und standardisierte gemeinsame ›Sprachen‹, sogenannte Übertragungsprotokolle, um die gegenseitige Erreichbarkeit sicherzustellen. Insbesondere das Internet Protocol (Internetprotokoll, kurz IP) hat eine zentrale Rolle. Das Internet ermöglicht den Transport beliebiger Daten.« Jens Tiemann/Gabriele Goldacker, *Vernetzung als Infrastruktur – Ein Internet-Modell*, Berlin: Kompetenzzentrum Öffentliche Informationstechnologie (ÖFIT), Oktober 2015, S. 10, <www.oeffentliche-it.de/documents/10181/14412/Vernetzung+als+Infrastruktur+-+Ein+Internet-Modell> (Zugriff am 5.2.2016).

6 Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland* [wie Fn. 4], S. 15; Hans-Jürgen Lange/ Astrid Bötticher (Hg.), *Cyber-Sicherheit*, Wiesbaden: Springer VS, 2015.

7 Das Due-Diligence-Prinzip geht auf ein Urteil des Internationalen Gerichtshofs zurück: International Court of Justice, *United Kingdom of Great Britain and Northern Ireland v. Albania, The Corfu Channel Case (Merits), Judgment of April 9th, 1949*, S. 4–38.

8 Siehe zur Übertragung des Konzepts auf die Cybersicherheit Scott Shackelford/Scott Russell/Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors*, Bloomington: Indiana University, 27.8.2015 (Kelley School of Business Research Paper No. 15-64).

rium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen.[9] Die Bundesregierung stellt in ihrer Cyber-Sicherheitsstrategie den präventiven und reaktiven Schutz der IT-Systeme und Infrastrukturen sowie zivile, polizeiliche und militärisch-defensive Ansätze in den Vordergrund. Zudem führt der Internationale Gerichtshof in einem Urteil aus, »dass die Verpflichtung zur Prävention eine Pflicht zur Sorgfalt« ist.[10] Due-Diligence-Pflichten ermöglichen es der internationalen Gemeinschaft, »Staaten für Versäumnisse bei der Absicherung ihrer Infrastruktur, für pflichtwidrig unterlassenes Einschreiten oder für mangelnde Kooperation bei der Abwehr und Aufklärung von Cyberattacken völkerrechtlich zur Verantwortung zu ziehen«.[11] Im Jahr 2000 hat die Generalversammlung der Vereinten Nationen Staaten dazu aufgefordert, »[to] ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies«.[12] Diese Idee hat die Gruppe der Regierungsexperten auf VN-Ebene (GGE), in der auch Deutschland vertreten ist, in ihren Abschlussbericht vom Juni 2015 aufgenommen. Alle Staaten sollen demnach sicherstellen, dass ihr Hoheitsgebiet, insbesondere dort befindliche oder sonst unter ihrer Kontrolle stehende Computersysteme und Infrastruktur, nicht zu Angriffen auf die Infrastruktur anderer Staaten missbraucht werden.[13]

»Due Diligence« wird in völkerrechtlichen Abhandlungen meist mit dem nicht unproblematischen Begriff Sorgfaltspflicht übersetzt.[14] Dieser verweist allerdings lediglich auf Restriktionen, denen das eigene Handeln unterliegt. Sinnvoller ist es, Due Diligence als »Sorgfaltsverantwortung« zu fassen. Der Due-Diligence-Grundsatz gewinnt nämlich seine besondere normative Kraft aus der Idee, dass Staaten nicht nur für die Einhaltung von Recht und Ordnung auf ihrem eigenen Territorium zuständig sind, sondern auch *Verantwortung für die externen Auswirkungen innerstaatlicher Regelungen* tragen. Einzelstaatliche Entscheidungen greifen immer häufiger über den innerstaatlichen Raum hinaus. Deshalb müssen Staaten Sorgfalt bei solchen Entscheidungen walten lassen und sich gegenseitig Rechenschaft darüber ablegen. Was den Schutz des Cyberraums anbelangt, wird in dieser Studie angenommen, dass Staaten sich nicht darauf beschränken dürfen, keine unverantwortlichen Entscheidungen zu treffen. Zudem wird unterstellt, dass dieser Schutz auch eine aktivierende und damit auf zwischenstaatliche Kooperation verweisende Dimension besitzt.[15] Demnach sind Staaten verpflichtet, zusammen mit anderen Staaten alles von ihnen vernünftigerweise Erwartbare zu tun, um ihren Beitrag zu einem »offenen, freien und sicheren Internet« zu leisten.

Diese Erwartung schließt ein, dass die Verfahren der Entscheidungsfindung hohen Standards genügen. Das heißt, verfügbare Kompetenzen sollen so weit wie möglich einbezogen und einseitige Interessenpolitik soll verhindert werden.[16] Cyber-Außen- und Sicherheitspolitik im Sinne der Sorgfaltsverantwortung schließt also die Art und Weise politischer Regulation notwendig ein. Die deutsche Cyber-Außen- und Sicher-

9 Michael N. Schmitt (Hg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013; Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland* [wie Fn. 4], S. 12.

10 International Court of Justice, »Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20.4.2010«, in: *ICJ Reports*, 79 (2010), S. 14–107. [Absatz 197]: »[...] the obligation [...] to prevent [...] is an obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party«.

11 Artikel 28ff der Artikelentwürfe der Völkerrechtskommission der Vereinten Nationen zur Staatenverantwortlichkeit: International Law Commission, »Responsibility of States for Internationally Wrongful Acts«, in: *Yearbook of the International Law Commission*, Bd. II, Teil 2, New York/Genf 2001, S. 26–143; veröffentlicht auch als Anhang zu United Nations General Assembly, *Responsibility of States for Internationally Wrongful Acts*, Resolution 56/83, New York, 12.12.2001.

12 United Nations General Assembly, *Combating the Criminal Misuse of Information Technologies*, Resolution 55/63, New York, 4.12.2000, <www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf> (Zugriff am 30.11.2015).

13 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, New York, Juni 2015.

14 Zum Völkerrecht des Netzes siehe Christian Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace*, Berlin: Stiftung Wissenschaft und Politik, Oktober 2014 (SWP-Studie 18/2014).

15 Als Vorbild kann die Kooperation von IT-Notfallteams (Computer Emergency Response Team, CERT) im Projekt CyberGreen (www.cybergreen.net) dienen. Hier arbeiten CERTs aus Staaten der Pazifikregion, auch aus Japan und China, zusammen, um für einen »grünen Cyberraum« zu sorgen. Ihr Selbstverständnis ist zwar strikt technisch, aber mit der Idee, gemeinsam Schwachstellen wie Schadsoftware oder anfällige Netzwerke zu identifizieren und zu bereinigen.

16 Ein Beispiel hierfür ist die Debatte um die Verschlüsselung von Kommunikation und divergierende Positionen von Sicherheitsbehörden auf der einen und Wirtschaftsvertretern auf der anderen Seite. Siehe hierzu auch Berklett Cybersecurity Project (Hg.), *Don't Panic: Making Progress on the »Going Dark« Debate*, Cambridge: Berkman Center for Internet and Society at Harvard, Februar 2016.

heitspolitik ist demzufolge europäisch zu koordinieren, zu militärischer Zurückhaltung verpflichtet sowie in inklusive und transparente Regelsetzungsprozesse einzubinden.[17]

- Zur Sorgfaltsverantwortung[18] gehört, dass Regelsetzungsprozesse ein hohes Maß an Repräsentativität und Inklusivität sowie Transparenz aufweisen müssen, denn »auf Dauer lässt sich in Demokratien keine Politik gegen den Willen der Mehrheit und nicht einmal gegen den Widerstand substantieller Teile der Minderheit durchsetzen. Gerade in Krisenzeiten ist der so genannte rally-effect ein unverzichtbares Element demokratischer Resilienz.«[19] Die Inklusivität von Rechtsetzungsprozessen sollte aber dort enden, wo privatwirtschaftliche Akteure beginnen, maßgeblichen Einfluss auf gesetzgebende Organe auszuüben.[20] Gegensteuern lässt sich nur mit transparenten und repräsentativen Verfahren, die auch anderen Staaten ein Mindestmaß an Gewissheit geben, dass ihre legitimen Interessen berücksichtigt werden. Die Offenheit eines politischen Systems ist wiederum eine wesentliche Bedingung dafür, dass Staaten einander vertrauen können, um in OSZE oder GGE ihren individuellen Beitrag zur Produktion des öffentlichen Gutes »sicherer Cyberraum« zu leisten. Diese Bedingungen sind alles andere als leicht zu erfüllen. In einem technisch anspruchsvollen Bereich wie der Cyber-Außen- und Sicherheitspolitik wird häufig verlangt, dass Beratungen vertraulich zu bleiben haben. Zudem dominiert hier fast zwangsläufig das Expertenwissen großer Konzerne, so dass zivilgesellschaftliche Interessenvertreter und Parlamentarier es außerordentlich schwer haben, als kompetente Gesprächspartner anerkannt zu werden. Darum sind besondere Anstrengungen nötig, um einseitige Interessenrepräsentanz und Instrumentalisierung der Politik durch die Wirtschaft zu verhindern.[21]

Eine Maxime des deutschen außenpolitischen Selbstverständnisses lautet, Regelsetzungen möglichst präzise mit den wichtigsten europäischen Partnern abzustimmen.[22] Wie die Außen- und Sicherheitspolitik ist auch der europäische Wirtschaftsraum durch digitale Technologien derart stark vernetzt, dass einzelstaatliche Maßnahmen wenig Sinn ergeben.

- Mit seiner Cyberaußenpolitik möchte Deutschland ein effektives Zusammenwirken für Cybersicherheit in Europa und weltweit erreichen. Deutsche Maßnahmen zur Förderung eines freien und sicheren Internets sollten daher immer europäisch oder transatlantisch eingebunden sein. Kein Staat kann ernsthaft beanspruchen, den globalen Cyberraum allein zu regulieren. Deutschland wird nur dann genügend Verhandlungsmacht auf der globalen Bühne gewinnen können, wenn es sich intensiv mit führenden Cybernationen in Europa (Frankreich, Großbritannien, Niederlande, Schweden, Italien, Spanien und Polen) abspricht und EU-Strukturen nutzt, etwa die Gruppe der Freunde der Präsidentschaft (Friends of the Presidency Group on Cyber Issues, FoP Cyber).[23] Nur mit europäisch abgestimmten Regelsetzungsprozessen lässt sich verhindern, dass sich die Krisensymptome der Integration im Zuge von Globalisierung und Digitalisierung verschärfen.

Für Deutschland ist es aus historischen Gründen selbstverständlich, jeglicher Militarisierung und Versicherheitlichung des Cyberraums[24] entgegenzuwirken.

17 Diese notwendigen Anforderungen beruhen auf den Ergebnissen der SWP-CyberLabs 2015 (siehe Fn. 3).

18 Zum Begriff der Verantwortung in den internationalen Beziehungen siehe die Ergebnisse der Tagung »Politik und Verantwortung« (Frankfurt/Main, 10.–12.2.2016), die 2017 in einem Sonderheft der Politischen Vierteljahresschrift (PVS) erscheinen sollen. Siehe auch Christopher Daase/Julian Junk (Hg.), *Internationale Schutzverantwortung – Normative Erwartungen und politische Praxis*, Sonderheft der Friedens-Warte, 88 (2013) 1–2; Hanns W. Maull, »What German Responsibility Means«, in: *Security and Human Rights*, 26 (2015), S. 11–24.

19 Daase, *Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik* [wie Fn. 1]. Unter »rally-effect« versteht man eine kurzfristige und weitgehende breite öffentliche Zustimmung zu bzw. Duldung von außergewöhnlichen Maßnahmen, vor allem in Krisenzeiten.

20 So gipfelte das Lobbying der Wirtschaftsunternehmen beim Entwurf der neuen EU-Datenschutzgrundverordnung (DSGVO) darin, dass ganze Textpassagen aus Positionspapieren von Wirtschaftsverbänden in den Änderungsvorschlägen zum Legislativakt wiederzufinden waren. Patrick Beuth, »Bundesregierung hofiert Lobbyisten«, in: *Zeit Online*, 10.3.2015, <www.zeit.de/digital/datenschutz/2015-03/eu-datenschutz grundverordnung-ministerrat-bundesregierung-lobbyplag> (Zugriff am 30.11.2015).

21 Liz Alderman, »Terror Threats Thaw Budgets Across Europe«, in: *New York Times*, 31.1.2016.

22 Eine empfehlenswerte Lektüre zum außenpolitischen Selbstverständnis Deutschland bietet Gunther Hellmann, »Germany's World. Power and Followship in a Crisis-Ridden Europa«, in: *Global Affairs*, 2016 (im Erscheinen).

23 Im Jahr 2013 wurde die FoP Cyber als ständige Einrichtung für drei Jahre geschaffen, um die Realisierung der europäischen Cybersicherheitsstrategie zu überwachen. Die Gruppe ist innerhalb der EU zum wichtigsten Forum dafür avanciert, alle Cyberthemen zu diskutieren und weiterzuverfolgen.

24 Siehe hierzu u.a. Ronald J. Deibert, *Black Code. Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart, 2013; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics. US*

Sorgfaltsverantwortung heißt auch, sich nicht nur an nationalen Interessen zu orientieren, sondern in den Kategorien globaler öffentlicher Güter zu denken. Deshalb ist es unerlässlich, die deutsche Tradition der Zivilmacht[25] auch in der Cyber-Außen- und Sicherheitspolitik fortzusetzen.

- Seit jeher folgt die Bundesrepublik dem Prinzip, ihre Interessen in der Regel mit ökonomischen und politischen statt mit militärischen Mitteln zu verfolgen. Angesichts dieser Tradition wäre allenfalls eine Cyber-Außen- und Sicherheitspolitik zu verantworten, die versucht, internationale Politik im Cyberraum zu zivilisieren. Das hieße, sozial akzeptierte Normen möglichst zu internationalisieren, etwa in der GGE, der OSZE und anderen Regierungsorganisationen und Foren, und auf diese Weise die gewaltsame Durchsetzung von Regeln zurückzudrängen. Militärische Gewalt – also auch eine offensive Cyberverteidigung[26], die auf Abschreckung baut – wäre national nur zur Selbstverteidigung sowie lediglich europäisch und parlamentarisch abgestimmt zu vertreten. Äußerst heikel wäre es, Cyberattacken mit automatischen Gegenangriffen und digitalen Vergeltungsschlägen zu beantworten. Zum einen nämlich wirft der Versuch, Cyberangriffe eindeutig zuzuordnen, allerlei technische, rechtliche und politische Fragen auf, zum anderen verursachen Gegenangriffe gravierende Nebenfolgen. Offensive Cyberverteidigung würde die Gefahr eines digitalen Rüstungswettlaufs (etwa durch Advanced Persistent Threats, APTs[27]) heraufbeschwören, mit unkalkulierbaren Konsequenzen für verwundbare kritische Infrastrukturen. Deshalb ist im Sinne der Sorgfaltsverantwortung eine Strategie der »Abschreckung durch Resilienz«[28] zu bevorzugen. Mit dem neuen IT-Sicherheitsgesetz und der Richtlinie zur Netz- und Informationssicherheit (Network and Information Security, NIS) gehen Deutschland und die EU mit gutem Beispiel voran, indem sie resiliente Informations- und Kommunikationsstrukturen in der kritischen Infrastruktur und Mindeststandards in der IT-Sicherheit schaffen. Im Sinne der Zivilisierung von Politik kommt der Resilienz-, der Präventions- sowie der Friedens- und Konfliktforschung eine Schlüsselrolle in der Cybersicherheit zu.

In der Sorgfaltsverantwortung verschmelzen materielle und prozedurale Inhalte zu einer übergreifenden Norm. Cybersicherheit im Sinne der Sorgfaltsverantwortung schließt auch eine bestimmte Form politischer Regulation ein. Es gilt, »der Versicherheitlichung des Internets und der Netzpolitik zu widerstehen. Ziel sollte nicht so sehr Sicherheit in abstracto sein, sondern eher Resilienz, d.h. Widerstandsfähigkeit gegen Schocks, und die ist nur durch komplexe gesamtgesellschaftliche Strukturen erreichbar«.[29] Der Cyber-Außen- und Sicherheitspolitik ist daher auch ein weites Sicherheitsverständnis zugrunde zu legen. Das wiederum heißt, dass alle Beteiligten in Staat, Wissenschaft, Wirtschaft und Gesellschaft gemeinsam ihre Verantwortung wahrnehmen müssen, was als Multistakeholder-Ansatz bezeichnet wird.[30]

Efforts to Secure the Information Age, London: Routledge, 2008; Myriam Dunn Cavelty, *Cyber-Security and the Negative Consequences of State Action*, Vortrag anlässlich der Konferenz »The Future of International Order«, in der Stiftung Wissenschaft und Politik, Berlin, 29.11.–1.12.2015.

25 Knut Kirste/Hanns W. Maull, »Zivilmacht und Rollentheorie«, in: *Zeitschrift für Internationale Beziehungen*, 3 (1996) 2, S. 283–312; Hanns W. Maull, »What German Responsibility Means«, in: *Security and Human Rights*, 26 (2015) 1, S. 11–24.

26 Offensive Strategien zielen darauf ab, »die Systeme anderer Staaten anzugreifen, sie zu sabotieren, die Kontrolle über sie zu erlangen, sie außer Kraft zu setzen oder Fehlfunktionen hervorzurufen [...]«. Es kommt aber darauf an, »durch sogenannte defensive Ansätze die eigenen IT-Strukturen, Kommunikations- und Waffensysteme zu sichern und aufrechtzuerhalten und sie vor Einwirkungen und Angriffen zu schützen.« Deutscher Bundestag, *Kleine Anfrage der Abgeordneten Dr. Alexander Neu u.a.: Krieg im »Cyber-Raum« – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung*, Drucksache 18/6496, Berlin, 16.10.2015. Zur Klassifizierung siehe auch Robert S. Dewar, *The »Triptych of Cyber Security«. A Classification of Active Cyber Defence*, Beitrag zur 6th International Conference on Cyber Conflict, Tallinn, 3.–6.6.2014.

27 APTs finden in Wellen statt. Nach der ersten Infiltrierung bleibt die Schadsoftware versteckt und greift in Etappen auf Daten zu. Ohne effektive Abwehrtools kann es Wochen oder gar Monate dauern, bis Sicherheitslücken und Angriffe überhaupt entdeckt werden. Siehe Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2015*, Bonn, November 2015, S. 26f.

28 Michael Rühle, »Das Prinzip Abschreckung«, in: *Frankfurter Allgemeine Zeitung*, 31.3.2015. Siehe auch Annegret Bendiek/Tobias Metzger, *Deterrence Theory in the Cyber-Century*, Berlin: Stiftung Wissenschaft und Politik, Mai 2015 (SWP EU/Europe Division Working Paper 2/2015).

29 Daase, *Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik* [wie Fn. 1].

30 Das Multistakeholder-Modell wurde auf der Weltkonferenz zur Informationsgesellschaft (WSIS II) in Tunis 2005 als Basis der Internet Governance festgelegt. Während des VN-Gipfels, der im Dezember 2015 im Zuge des WSIS-Folgeprozesses stattfand, wurde darüber gestritten, inwiefern das beim Internet Governance Forum (IGF) und bei der Internet Corporation for Assigned Names and Numbers (ICANN) erfolgreich praktizierte Modell weiter ausgestaltet werden kann.

Sorgfaltsverantwortung in der institutionellen Praxis

Die deutsche Politik trägt der Norm der Sorgfaltsverantwortung ansatzweise schon heute Rechnung, doch diese ist institutionell noch nicht ausreichend verankert. Aus diesem Blickwinkel sind Kohärenz und inhaltliche Konsistenz der deutschen Cyber-Außen- und Sicherheitspolitik auf den Prüfstand zu stellen. Deren aktuelle institutionelle Struktur spiegelt wider, dass bereits ein weiter Weg bei der Umsetzung der Sorgfaltsverantwortung gegangen wurde. Die zuständigen Behörden sind mittlerweile eng verflochten, aber klar ist auch, dass im Hinblick auf europäische Zusammenarbeit, Inklusivität und Zivilität noch einiges verbessert werden muss.

Institutionelle Strukturen

Die Bundesregierung hat sich verpflichtet, ein mit den zuständigen staatlichen Stellen abgestimmtes und vollständiges Instrumentarium für die Abwehr von Angriffen aus dem Cyberraum zu schaffen.[31] Es soll dazu beitragen, die gesamtstaatliche Sicherheitsvorsorge zu gewährleisten. Die Entwicklung ausdifferenzierter Zuständigkeiten ist politisch gewollt.[32] In der deutschen Cyber-Außen- und Sicherheitspolitik findet sich eine ganze Reihe von Kooperationen, die sich im Wesentlichen auf fünf Pfeiler stützen.

Erster Pfeiler: Bundesamt für Sicherheit in der Informationstechnik

Die ministerielle Federführung in Deutschland in Fragen der Cybersicherheit liegt beim Bundesministerium des Innern (BMI).[33] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der wichtigste IT-Sicherheitsdienstleister des Bundes und dem BMI nachgeordnet. Auch ist das BSI für die operative Abwehr von Angriffen auf die IT-Infrastruktur des Bundes verantwortlich. Dafür steht ihm ein IT-Notfallteam (CERT-Bund) zur Verfügung. Das Bundesamt erfüllt den gesetzlichen Auftrag als »zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes«, zuständig für die »Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes«, für die »Vorgabe von Sicherheitsstandards« sowie für Zertifizierungen.[34] Wegen der hohen Qualität des BSI-Standards (ISO 27001) zur Förderung zertifizierter Basisfunktionen und aufgrund anderer Empfehlungen genießt das Bundesamt große europäische und internationale Anerkennung. Seit Jahren betreibt es einen intensiven internationalen Erfahrungs- und Informationsaustausch auf Leitungs- und Fachebene. Auf der operativen Ebene ist vor allem die Kooperation mit anderen IT-Notfallteams wichtig. CERT-Bund ist Teil des interdisziplinär ausgerichteten Warn- und Alarmierungsverbunds (International Watch and Warning Network, IWWN).[35] Auf innerstaatlicher Ebene hat das BSI die Gründung der Allianz für Cybersicherheit angestoßen, die mittlerweile das Know-how zur Cybersicherheit in Deutschland bündelt und zur Hauptanlaufstelle für Unternehmen und Bürger geworden ist.[36] Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und das IT-Notfallteam der Bundeswehr (CERTBw) arbeiten eng mit dem BSI zusammen, speziell mit dessen IT-Lage- und Analysezentrum und dem CERT-Bund.

31 Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland* [wie Fn. 4].

32 In Norwegen beispielsweise liegt die nationale Cybersicherheitsstrategie im Geschäftsbereich des Justizministeriums. Das norwegische Außenministerium erarbeitet zurzeit eine globale Strategie für den Cyberraum.

33 Bundesministerium der Verteidigung, *Weißbuch 2016*, <www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pNyydL3y1Mzi4qTS5Az9gmxHRQBg2ftX/> (Zugriff am 30.11.2015).

34 Bundesministerium der Justiz und für Verbraucherschutz (Hg.), *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)*, zuletzt geändert am 17.7.2015, <www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html> (Zugriff am 30.11.2015).

35 IT Law Wiki, *International Watch and Warning Network*, <http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network> (Zugriff am 30.11.2015).

36 Bundesamt für Sicherheit in der Informationstechnik, *Allianz für Cyber-Sicherheit*, <www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html> (Zugriff am 30.11.2015).

Zweiter Pfeiler: Nationales Cyber-Abwehrzentrum
Ein wichtiger Schritt auf dem Weg zur Umsetzung der Sorgfaltsverantwortung bestand darin, 2011 ein nationales Cyber-Abwehrzentrum ins Leben zu rufen.[37] Die Informationsplattform soll die Zusammenarbeit zwischen den Behörden vereinfachen sowie Schutz- und Abwehrmaßnahmen gegen IT-Angriffe verbessern. Darüber hinaus ist das Abwehrzentrum Bestandteil der projektbasierten Zusammenarbeit mit Firmen und Dienstleistern sowie mit Sicherheitsbehörden im Ausland. Das Trennungsgebot, ein Grundsatz bundesdeutschen Rechts, sieht vor, dass Aufgaben der Polizei und der Nachrichtendienste durch unterschiedliche, organisatorisch voneinander getrennte Behörden wahrgenommen werden müssen. Für die Spionageabwehr ist das BfV zuständig, während dem BKA die polizeiliche Verfolgung kriminell motivierter IT-Angriffe obliegt. Die Abteilung Technische Aufklärung (TA) des Bundesnachrichtendienstes betreibt Informationsgewinnung mit technischen Mitteln (Signals Intelligence, SIGINT), beschafft gemäß ihrem gesetzlichen Auftrag Informationen von außen- und sicherheitspolitischer Bedeutung und wertet diese aus.[38] Mit diesen Informationen unterstützt der BND auch die Bundeswehr bei der Cyberverteidigung.

Dritter Pfeiler: Nationaler Cyber-Sicherheitsrat
Beim Umgang mit den Herausforderungen der Cybersicherheit soll eine starke gesamtstaatliche Koordination gewährleistet bleiben.[39] Zu diesem Zweck versammeln sich im Nationalen Cyber-Sicherheitsrat ressortübergreifend die Staatssekretäre unter dem Vorsitz des Beauftragten der Bundesregierung für Informationstechnik.[40] IT-Sicherheit ist in der Bundesrepublik zudem eine föderale Aufgabe. Gebildet wird der Cyber-Sicherheitsrat aus zwei Ländervertretern, Repräsentanten mehrerer Bundesbehörden – Bundesministerium des Innern, BKA, Auswärtiges Amt (AA), Bundesministerium für Bildung und Forschung, Bundesministerium der Verteidigung (BMVg), Bundesministerium für Wirtschaft und Energie (BMWi), Bundesministerium der Justiz und für Verbraucherschutz sowie Bundesministerium der Finanzen – und vier assoziierten Vertretern der Wirtschaft (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien, Bundesverband der Deutschen Industrie, Deutscher Industrie- und Handelskammertag, Übertragungsnetzbetreiber Amprion GmbH). Der Cyber-Sicherheitsrat tagt seit 2011 dreimal jährlich. Grundsätzliche Fragen der IT-Steuerung und -Sicherheit des Bundes werden außerdem im ressortübergreifenden Rat der IT-Beauftragten (auch IT-Rat) behandelt.

Vierter Pfeiler: Cyber-Außenpolitik
Die deutsche Cybersicherheitsstrategie von 2011 sieht vor, eine zielgerichtete und koordinierte Cyber-Außenpolitik zu entwickeln, um präventive Maßnahmen für die IT-Sicherheit in Deutschland ergreifen zu können, insbesondere zum Schutz kritischer Infrastrukturen und in der internationalen Zusammenarbeit.[41] Die Cyber-Außenpolitik schließt ein, dass deutsche Interessen in der EU, internationalen Organisationen und Gremien sowie bilateralen Dialogen vertreten werden. Das Auswärtige Amt hat 2011 einen Koordinierungsstab für Cyber-Außenpolitik geschaffen.[42] Er soll als Schnittstelle zwischen nationalen Ressortpolitiken auf der einen und der Koordination internationaler Einflussnahme auf der anderen Seite dienen, um ein Klima der Sicherheit und des Vertrauens zu schaffen, denn dieses ist für eine defensive Cybersicherheitsstrategie unverzichtbar.

37 Darin vertreten sind das BSI, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND), das Bundeskriminalamt (BKA), das Zollkriminalamt (ZKA), die Bundespolizei (BPol) und die Bundeswehr. Bundesministerium des Innern, *Nationales Cyber-Abwehrzentrum*, <www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberabwehrzentrum/cyberabwehrzentrum_node.html> (Zugriff am 22.2.2016).
38 Zur Umsetzung der sogenannten Strategischen Initiative Technik (SIT), einem technischen Modernisierungsprogramm, hat der Haushaltsausschuss des Bundestages dem Bundesnachrichtendienst 2014 laut Medienberichten insgesamt 300 Millionen Euro zur Verfügung gestellt. Durch die Auszahlung jährlicher Tranchen sollen so bis 2020 die Fähigkeiten der technischen Aufklärung des BND ausgebaut werden. John Goetz/Hans Leyendecker, »Aufrüsten für den Cyberkampf«, in: *Süddeutsche Zeitung*, 10.11.2014, <www.sueddeutsche.de/digital/bundesnachrichtendienst-aufruesten-fuer-den-cyberkampf-1.2211761> (Zugriff am 5.2.2016).
39 Carsten Köppl, *IT-Sicherheit föderalisiert sich*, Fazit zum Kongress »Public IT-Security« (PITS), Berlin, 25./26.9.2013, <www.public-it-security.de/icc/public/nav/e86/e862fd19-3c66-6413-ccca-2a307b988f2e.htm>.
40 Bundesministerium des Innern, *Cyber-Sicherheitsrat*, <www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cybersicherheitsrat/cybersicherheitsrat_node.html> (Zugriff am 22.2.2016).
41 Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland* [wie Fn. 4].
42 Auswärtiges Amt, *Cyber-Außenpolitik*, <www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html> (Zugriff am 5.2.2016).

Fünfter Pfeiler: Bundeswehr

Die Maßnahmen der Bundeswehr sollen sich auf den Schutz ihrer eigenen Handlungsfähigkeit gemäß der zugrunde liegenden Mandatierung beschränken, »um auf diese Weise Cybersicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern«.[43] Hierfür sind die CNO-Kräfte[44] der Bundeswehr zuständig, die weiter ausgebaut und künftig zur aktiven Cyberverteidigung eingesetzt werden sollen.[45] Das deutet auf einen möglichen Paradigmenwechsel von der defensiven hin zur offensiven Cyberverteidigung hin. So bekräftigte Verteidigungsministerin Ursula von der Leyen im September 2015, es werde »ein neues Zielbild für die Bereiche Cyber-Raum und IT im nachgeordneten Bereich und im Ministerium entwickelt«.[46] Für präzise militärische Cyberoperationen ist derzeit der Aufbau eines Pools von IT-Reservisten in Planung. Außerdem soll der Militärische Abschirmdienst (MAD) im Auslandseinsatz einen erweiterten Abschirmauftrag erhalten, der sich auf alle Personen erstrecken soll, die Sicherheit und Einsatzbereitschaft der Truppe gefährden können.[47] Laut dem Ständigen Vertreter des Präsidenten des MAD, Oberst Joachim Smola, sei der MAD »weit mehr [...] als ein rein abwehrender Nachrichtendienst«, sondern ein »umfassender Serviceleister in Belangen der Sicherheit und begleite die Bundeswehr [...] sowohl an den Standorten in Deutschland als auch im Auslandseinsatz«.[48]

Auf parlamentarischer Ebene werden wesentliche Bereiche der Cyber-Sicherheitsstrategie, welche die geheimdienstlichen Tätigkeiten der Bundesregierung betreffen, von zwei maßgeblichen Gremien kontrolliert: dem Parlamentarischen Kontrollgremium (PKGr) und dem NSA-Untersuchungsausschuss. In den Fachausschüssen – Ausschuss Digitale Agenda, Innenausschuss, Auswärtiger Ausschuss, Verteidigungsausschuss – werden weitere Themen einer Cyber-Außen- und Sicherheitspolitik behandelt. Der Cyberraum kennt keine Trennung zwischen Innen- und Außenpolitik. Dieser Erkenntnis sollte die für die Demokratie und Rechtsstaatlichkeit notwendige begleitende parlamentarische Arbeit konzeptionell und institutionell Rechnung tragen. Innenpolitische Anpassungen wären im Sinne der Sorgfaltsverantwortung umzusetzen. Nur so lässt sich das Vertrauen wiederherstellen, das bei Bürgern, Verbündeten und EU-Partnern im Zuge der Enthüllungen Edward Snowdens verloren gegangen ist. Vertrauen ist unabdingbare Voraussetzung für europäische Kooperation und Politik. Die Erfüllung der drei wichtigen Anforderungen an eine Cyber-Außen- und Sicherheitspolitik – nämlich europäische Zusammenarbeit, Inklusivität, Zivilität – lässt allerdings noch zu wünschen übrig:

Europäische Zusammenarbeit

Unbefriedigend sind die Verfahren auf Bundes- und EU-Ebene, mit denen ein Lagebild zu den Bedrohungen im Cyberraum erstellt werden soll. Um die Strafverfolgung zu verbessern, wird vorgeschlagen, das Nationale Cyber-Abwehrzentrum in ein übergeordnetes Gremium für IT-Sicherheit zu verwandeln (vergleichbar mit dem Gemeinsamen Terrorismusabwehrzentrum), denn bisher vereint es nicht alle Bundes- und Landesbehörden. Auch im Hinblick auf einen europäischen Informationsaustausch wird mehr Kooperation zwischen Behörden auf nationaler und auf EU-Ebene verlangt.[49] Wichtige Partner Deutschlands wie Frankreich oder die Niederlande bemängeln, oft sei nicht nur unklar, was »die deutsche Position«

43 Bundesministerium des Innern (Hg.), *Cyber-Sicherheitsstrategie für Deutschland* [wie Fn. 4].

44 Computernetzwerkoperationen (CNO) sind nicht-kinetische Angriffsmittel, die ihre Wirkung durch den Einsatz von Computercodes oder Computerprogrammen im Cyberraum entfalten. Sie dienen der Manipulation, Störung oder gar Zerstörung gegnerischer Informations- und Kommunikationssysteme ebenso wie dem Schutz eigener Systeme oder der gezielten Informationsgewinnung aus nicht öffentlich verfügbaren Datenquellen. CNO werden daher unterschieden in Computer Network Attacks (CNA), Computer Network Defense (CND) und Computer Network Exploitation (CNE).

45 Bundesministerium der Verteidigung, *Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig*, Berlin, 17.9.2015.

46 Ebd.

47 Andre Meister, »Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr ›Cyberwar‹ und offensive digitale Angriffe«, *netzpolitik.org*, 30.7.2015, <https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/> (Zugriff am 30.11.2015).

48 »Geheimhaltung versus Transparenz«, in: *Behörden Spiegel*, November 2015, S. 48.

49 Im Geschäftsbereich des Europäischen Auswärtigen Dienstes besteht seit 2011 das EU Intelligence Analysis Centre (EU INTCEN), das auf der Basis von Zulieferungen durch nationale Nachrichtendienste zivile Lageanalysen für EU-Entscheidungsträger erstellt. European External Action Service, *EUINTCEN Fact Sheet*, Brüssel, 5.2.2015, <http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf> (Zugriff am 5.2.2016.)

eigentlich vorsehe, sondern auch, mit welchem Ministerium in der europäischen Abstimmung zu verhandeln sei. Zudem ist die notwendige europäische Koordinierung schwerfällig, was auch an der äußerst komplizierten Ressortzuständigkeit liegt. Seit der Bundestagswahl 2013 diskutieren die Koalitionspartner, ob Deutschland ein Internetministerium oder eine sogenannte Digitalagentur[50] brauche. Sie konnten sich aber nur auf ein Amt ohne Macht und Ressourcen einigen, den Posten der Internetbotschafterin der Bundesregierung, derzeit besetzt mit Gesche Joost.

Inklusivität

Nachgelagerte Behörden wie BSI, BKA und BND haben bereits grundlegende institutionelle Anpassungen zur Abwehr von Cyberangriffen vorgenommen. Teilweise sind diese Reformen nur durch die unautorisierte Veröffentlichung von Dokumenten bekannt geworden.[51] Die vieldiskutierte starke institutionelle Abhängigkeit des BSI bleibt indes bestehen.[52] So hat das Bundeskabinett den Vorsitzenden des Cybersicherheitsrats e.V., Arne Schönbohm, im Februar 2016 zum BSI-Präsidenten ernannt. In der Öffentlichkeit werden seine Verbindungen zur IT- und Rüstungswirtschaft argwöhnisch beäugt. Auch weisen kritische Stimmen darauf hin, »dass der ›Angreiferseite‹ im Vergleich zu den ›Verteidigern‹ der IT-Sicherheit die sechs- bis zehnfachen Ressourcen für Cyberattacken und für die Kompromittierung der IT-Sicherheit zur Verfügung stehen«.[53] Außerdem greife nur jedes fünfte Unternehmen auf IT-Beratung durch staatliche Stellen zurück, so Susanne Dehmel, Mitglied der Geschäftsleitung des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom).[54] Ferner würden sich Unternehmen, die Opfer von Cyberangriffen geworden seien, eher an die Verfassungsschutzämter als an die Polizei wenden, da diese verpflichtet sei, bei einer möglichen Straftat ein Ermittlungsverfahren einzuleiten. Eine Reform der Nachrichtendienste sowie eine verbesserte parlamentarische Kontrolle der Dienste durch das PKGr befinden sich zwar in der Beratung, doch ist noch nicht abzusehen, ob der NSA-Untersuchungsausschusses seine Arbeit überhaupt erfolgreich abschließen kann.[55] Die von der Bundesregierung eingesetzte Sachverständige Vertrauensperson, Kurt Graulich, prüfte zwar die sogenannten Selektorenlisten der NSA, die an den BND weitergegeben worden waren. Die Ergebnisse lassen aber weiterhin viele Fragen offen. Hansjörg Geiger, ehemaliger BfV- und BND-Präsident, hat sich 2015 dafür ausgesprochen, einen Kodex für den nachrichtendienstlichen Informationsaustausch zu formulieren und den Posten eines Nachrichtendienstbeauftragten nach dem Vorbild des Wehrbeauftragten zu schaffen.[56]

Zivilität

Der Staatssekretär im Bundesinnenministerium und IT-Beauftragte der Bundesregierung, Hans-Georg Engelke, hat zwar betont, eine behördliche Zusammenarbeit bei der IT-Sicherheit sei notwendig, aber die ministerielle Federführung in Fragen der Cybersicherheit liege beim BMI. Dieser Anspruch wird jedoch im Zuge der Weißbuchdiskussion 2016 bereits in Frage gestellt. Das Problem der zuweilen ineffizienten Ressortzuständigkeit konnte auch der Nationale Cyber-Sicherheitsrat noch nicht beseitigen. Im Zuge der Aufklärung der NSA-Affäre hat die Bundesregierung zwar im Juli 2013 ein Acht-Punkte-Programm

50 Bundesministerium für Wirtschaft und Energie, *Digitale Strategie 2025*, Berlin, März 2016.

51 Daraufhin eröffnete Generalbundesanwalt Harald Range wegen Verdachts auf Landesverrat ein Ermittlungsverfahren gegen das Internetportal *netzpolitik.org*. Das Verfahren wurde indes nach politischer Intervention eingestellt. Siehe »Maas zweifelt an Verfahren gegen ›netzpolitik.org‹«, in: *Zeit Online*, 31.7.2015, <www.zeit.de/digital/internet/2015-07/netzpolitik-ermittlungen-journalisten-innenministerium-maassen> (Zugriff am 30.11.2015).

52 Trotz anderslautender Medienberichte – siehe etwa »Bundesamt für Sicherheit in der Informationstechnik (BSI) soll neue Bundesbehörde werden«, in: *Der Spiegel*, 10.8.2014 – ist das BSI weiterhin dem BMI unterstellt. Siehe *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), § 1 Bundesamt für Sicherheit in der Informationstechnik*.

53 Ingo Ruhmann, »Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht«, in: *Kriegführung im Cyberspace*, Beilage zu *Wissenschaft und Frieden*, (2015) 3, S. 12–16 (Dossier Nr. 79).

54 Bundesministerium der Verteidigung, *Weißbuchprozess: Bundeswehr sucht Dialog mit Cyber-Community*, Berlin, 18.9.2015.

55 Thomas Oppermann/Christian Flisek/Burkhard Lischka, *Rechtsstaat wahren – Sicherheit gewährleisten!*, Berlin: SPD-Bundestagsfraktion, 16.6.2015, <www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf> (Zugriff am 30.11.2015).

56 Rudi Wais, »So könnte eine bessere Kontrolle der Nachrichtendienste aussehen«, in: *Augsburger Allgemeine*, 3.5.2015, <www.augsburger-allgemeine.de/politik/So-koennte-eine-bessere-Kontrolle-der-Nachrichtendienste-aussehen-id33933952.html> (Zugriff am 30.11.2015).

zum besseren Schutz der Privatsphäre veröffentlicht.[57] Zu fragwürdigen Praktiken der Geheimdienste, etwa zur Industriespionage[58] und dem Führen sogenannter Selektorenlisten mit Ausspähzielen[59], bezog der Cyber-Sicherheitsrat aber öffentlich nicht Stellung und schwieg auch zur Cyberattacke auf den Bundestag. Gerade zum Angriff auf das höchste Verfassungsorgan Deutschlands hätten viele Beobachter eine angemessene Reaktion erwartet.

Digitale Industriepolitik und die Bedeutung privater Akteure

Sorgfaltsverantwortung erfordert nicht nur den Aufbau institutioneller Strukturen, sondern auch anspruchsvolle Kapazitäten in der Informations- und Kommunikationstechnologie (IKT) und deren »intelligente Vernetzung«.[60] Während der letzten Jahrzehnte hat sich die deutsche Wirtschaft in der Automatisierung unter dem globalen Wettbewerbs- und Innovationsdruck gut behauptet. Überdies will das Bundeswirtschaftsministerium mit der Digitalen Strategie 2025 die kleinen und mittleren Unternehmen fördern. In der Cyber-Außen- und Sicherheitspolitik der Bundesregierung spielen private Akteure eine außerordentlich wichtige Rolle. Industriestandorte gewinnen an strategischer Bedeutung. Die dort ansässigen Unternehmen schaffen nicht nur Arbeitsplätze und Mehrwert, sondern setzen Maßstäbe für die Wettbewerbsfähigkeit ganzer Volkswirtschaften.[61] Die Bundesregierung ist der Auffassung, dass noch reichlich ungenutzte Potentiale in der deutschen IKT liegen, denn laut einer Studie des Fraunhofer-Instituts für System- und Innovationsforschung können intelligente Netze einen gesellschaftlichen Gesamtnutzen von 56 Milliarden Euro pro Jahr erzeugen.[62]

Bei der Digitalisierung sind jedoch andere Länder erfolgreicher. Vorreiter sind überwiegend amerikanische, südkoreanische und chinesische Firmen. Die Bundesregierung hat 2014 die Programme Digitale Agenda und Digitale Verwaltung aufgelegt, mit denen sie global Anschluss zu finden hofft. Dafür sind sie allerdings recht mager ausgestattet, verglichen mit Programmen der US-Regierung zur Förderung von Forschungsprojekten, etwa zur Entwicklung von Quantencomputern oder Big-Data-Analysefähigkeiten. Das Zukunftsprojekt Industrie 4.0 wird auf Bundesebene mit rund 200 Millionen Euro aus Mitteln von BMBF und BMWI finanziert. Das reicht jedoch bei weitem nicht aus, um konkurrenzfähig zu werden. Festzuhalten ist, dass in der sich entwickelnden digitalen Industriepolitik öffentlich-private Kooperation, eine Einbindung in die europäische Harmonisierung sowie die Ausrichtung auf defensive Cyber-Sicherheitspolitik nötig sind, um der Sorgfaltsverantwortung Genüge zu tun.

Europäische Zusammenarbeit

Aus der Wissenschaft wurde Kritik laut, »der Diskurs zu Industrie 4.0 [verlaufe] häufig zu technisch und national«.[63] Daher sei dieser Diskurs stärker als bisher mit der EU-Ebene zu verzahnen, denn bei (kritischen) Infrastrukturen würden Lösungen zu Datensicherheit, Betriebssicherheit und Datenschutz nicht zusammengeführt.[64] Das spiegelt sich auch im Programm Digitale

57 Bundesministerium des Innern/Bundesministerium für Wirtschaft und Technologie, *Maßnahmen für einen besseren Schutz der Privatsphäre*, Fortschrittsbericht, Berlin, 14.8.2013, <www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2013/08/bericht.pdf?__blob=publicationFile>.

58 Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion Die Linke. Geheimdienstliche Angriffe und Spionage bei deutschen Unternehmen*, Drucksache 18/2281, Berlin, 5.8.2014.

59 Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD. Abhörprogramme der USA und Umfang der Kooperation der deutschen Nachrichtendienste mit den US-Nachrichtendiensten*, Drucksache 17/14560, Berlin, 14.8.2013; Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Christine Buchholz, Ulla Jelpke, weiterer Abgeordneter und der Fraktion Die Linke. Aktivitäten der Bundesregierung zur Aufklärung der NSA-Ausspähmaßnahmen und zum Schutz der Grundrechte*, Drucksache 18/159, Berlin, 12.12.2013; Deutscher Bundestag, *Hitzige Debatte über die BND-NSA-Kooperation*, Berlin, 21.5.2015, <www.bundestag.de/dokumente/textarchiv/2015/kw21_de_aktuelle_stunde_nsa/375278> (Zugriff am 5.2.2016).

60 Deutscher Bundestag, *Unterrichtung durch die Bundesregierung. Strategie Intelligente Vernetzung*, Drucksache 18/6022, Berlin, 18.9.2015, <http://dip21.bundestag.de/dip21/btd/18/060/1806022.pdf> (Zugriff am 30.11.2015).

61 Initiative D21 (Hg.), *D21-Digital-Index 2015. Die Gesellschaft in der digitalen Transformation*, Berlin 2015.

62 Deutscher Bundestag, *IKT-Potenziale nicht ausgeschöpft*, Berlin, 2.10.2015, <www.bundestag.de/presse/hib/2015_10/-/390352> (Zugriff am 30.11.2015).

63 Sabine Pfeiffer, »Industrie 4.0 und die Digitalisierung der Produktion – Hype oder Megatrend?«, in: *Aus Politik und Zeitgeschichte*, 65 (2015) 31–32, S. 6–12.

64 So Peter Liggesmeyer, Leiter des Fraunhofer-Instituts für

Agenda 2014–2017 der Bundesregierung wider. Zu den dort skizzierten sieben Handlungsfeldern gehört die »europäische und internationale Dimension«.[65] Laut Koalitionsvertrag soll zwar ein »europäischer Vertrauensraum« geschaffen werden[66], aber vorrangig mit Hilfe nationaler »Maßnahmen zur Rückgewinnung der technologischen Souveränität«.[67] Ungewiss ist, wie dieser offenkundige Widerspruch aufgelöst werden soll. Nationale IT-Gipfel sind von Interessen dominiert, hinter denen gut organisierte, kapitalkräftige und mit umfassender Kompetenz ausgestattete Akteure stehen. Deren Augenmerk gilt zuvorderst der nationalen Industriepolitik. Doch die Industrie 4.0, das Internet der Dinge, kann nur europäisch, wenn nicht sogar nur global gestaltet werden.[68]

Die Europäische Kommission hat im Mai 2015 eine Strategie für den digitalen Binnenmarkt vorgelegt.[69] Von dessen Vollendung verspricht sie sich einen Beitrag von 520 Milliarden Euro zum Bruttoinlandsprodukt der EU-Staaten. Allerdings stehen der Kommission derzeit nur sehr begrenzte Mittel für die Entwicklung digitaler Schlüsseltechnologien zur Verfügung. Für die IKT-Förderung sind aus dem Finanztopf der Connecting Europe Facility (CEF) rund eine Milliarde Euro für die Mitgliedstaaten vorgesehen, verteilt über sieben Jahre. Im Forschungsbereich stehen 7,2 Milliarden Euro (2014–2020) für die EU-28 aus dem Finanzprogramm Horizon 2020 bereit.[70] Die Industriepolitik 4.0 auf EU-Ebene wird seit Antritt der Juncker-Kommission im November 2014 mit Hilfe eines umfangreichen Gesetzespakets zum digitalen Binnenmarkt ausgebaut. Marktschaffende, marktregulierende und distributive Politiken sollen nach Ansicht der Kommission möglichst zügig auf den Weg gebracht werden. Das geforderte Tempo ist jedoch ein Problem, denn die Kommission muss die Rechtspolitiken sämtlicher 28 Mitgliedstaaten harmonisieren. Als wichtige Wegmarken einer europäischen beziehungsweise transatlantischen Verständigung in Datensicherheit und Datenschutzpolitik gelten einige Grundsatzurteile des Europäischen Gerichtshofs (EuGH) aus den Jahren 2014 und 2015, nämlich zur Illegalität der Vorratsdatenspeicherung, zum Recht auf Vergessen und zur Unwirksamkeit des Safe-Harbor-Abkommens.[71] Dessen Nachfolgevereinbarung zwischen EU und USA, der sogenannte Privatsphäre-Schutzschirm (Privacy Shield), ist hier ebenfalls hervorzuheben.[72] Des Weiteren haben sich Parlament, Rat und Kommission Ende Dezember 2015 auf eine Datenschutzgrundverordnung sowie eine Richtlinie zur Netz- und Informationssicherheit geeinigt.[73]

Experimentelles Software Engineering und Präsident der Gesellschaft für Informatik, im Ausschuss Digitale Agenda, siehe »Umfassende Sicherheit für Industrie 4.0«, in: *heute im bundestag*, Nr. 345, 1.7.2015.

65 Bundesministerium für Wirtschaft und Energie/Bundesministerium des Innern/Bundesministerium für Verkehr und digitale Infrastruktur (Hg.), *Digitale Agenda 2014–2017*, Berlin, August 2014, <www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6> (Zugriff am 30.11.2015).

66 *Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode*, Berlin, 27.11.2013, <www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile> (Zugriff am 30.11.2015).

67 Ebd., S. 147.

68 Deutscher Bundestag, *Antrag der Fraktionen der CDU/CSU und SPD, Industrie 4.0 und Smart Services – Wirtschafts-, arbeits-, bildungs- und forschungspolitische Maßnahmen für die Digitalisierung und intelligente Vernetzung von Produktions- und Wertschöpfungsketten*, Drucksache 18/6643, Berlin, 10.11.2015, S. 3; Ansgar Baums/Martin Schössler/Ben Scott (Hg.), *Kompendium Industrie 4.0. Wie digitale Plattformen die Wirtschaft verändern – und wie die Politik gestalten kann*, Berlin, Oktober 2015.

69 Europäische Kommission, *Strategie für einen digitalen Binnenmarkt für Europa*, COM(2015) 192 final, Brüssel, 6.5.2015, <http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=DE> (Zugriff am 30.11.2015).

70 European Commission, *Horizon 2020. The EU Framework Programme for Research and Innovation*, <https://ec.europa.eu/programmes/horizon2020/> (Zugriff am 30.11.2015); Eric Maurice, »China to Join Juncker's Investment Scheme«, in: *EU Observer*, 28.9.2015.

71 Europäischer Gerichtshof, *Urteil des Gerichtshofs: »Elektronische Kommunikation – Richtlinie 2006/24/EG – Öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze – Vorratsspeicherung von Daten, die bei der Bereitstellung solcher Dienste erzeugt oder verarbeitet werden – Gültigkeit – Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union«*, Luxemburg, 8.4.2014, <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=DE> (Zugriff am 30.11.2015); Gerichtshof der Europäischen Union, *Der Betreiber einer Internetsuchmaschine ist bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich*, Pressemitteilung Nr. 70/14, Luxemburg, 13.5.2014; Gerichtshof der Europäischen Union, *Der Gerichtshof erklärt die Entscheidung der Kommission, in der festgestellt wird, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten, für ungültig*, Pressemitteilung Nr. 117/15, Luxemburg, 6.10.2015.

72 Annegret Bendiek/Evita Schmieg, *EU-Außenhandel und Datenschutz. Wie lässt sich beides besser vereinbaren?* Berlin: Stiftung Wissenschaft und Politik, Februar 2016 (SWP-Aktuell 10/2016).

73 European Parliament, *Personal Data Protection: Processing and Free Movement of Data (General Data Protection Regulation)*, Procedure File 2012/0011(COD), <www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011(COD)> (Zugriff am 30.11.2015).

Industrievertreter hingegen ziehen mit Blick auf die europäische Harmonisierung eine kritische Bilanz. In den Urteilen des EuGH und den Gesetzesinitiativen der Kommission sehen sie eine »Inanspruchnahme von Politikfeldern für eine digitale Industriepolitik«[74], im Klartext also eine protektionistische Politik.

Inklusivität

Die Bedeutung privater Akteure lässt sich auch daran ablesen, dass sie viele kritische Infrastrukturen wie etwa Krankenhäuser, Banken, Energieunternehmen und Wasserwerke betreiben. Private Akteure verfügen zudem oftmals über relevantes Wissen für die Einschätzung von Bedrohungslagen und die Entwicklung von Instrumenten zur Gefahrenabwehr. Nur Banken wissen, wie oft sie angegriffen werden, und ohne Informationen von Industrieunternehmen über Spionage kann kein Nachrichtendienst sinnvolle Gegenmaßnahmen ergreifen. Jede Regelsetzung, Entwicklung von Standards und Politikformulierung sollte daher im Schulterschluss mit der Privatwirtschaft erfolgen, möglichst in Public-Private Partnerships (PPP). Der Schutz kritischer Infrastrukturen zum Beispiel wurde in Deutschland 2007 in Form des UP KRITIS eingeführt, einer öffentlich-privaten Partnerschaft von Betreibern solcher Infrastruktur.[75] Auf EU-Ebene hat die Kommission 2013 einen Richtlinienentwurf zur Netz- und Informationssicherheit vorgestellt. Die Richtlinie soll die IT bei Betreibern kritischer Infrastrukturen und großen Online-Dienstleistern sicherer machen und wird die betroffenen Firmen verpflichten, Sicherheits- und Datenschutzvorfälle sowie IT-Angriffe zu melden. Die Auflagen sollen für sämtliche Betreiber und Anbieter »essentieller Dienste« gelten, etwa in den Bereichen Energie, Wasserversorgung, Transport, Finanzwesen, Gesundheit und Internet. Im Entwurf werden Verkehrsknoten, Domain-Regierungsstellen, Online-Marktplätze und Suchmaschinen aufgeführt, nicht aber soziale Netzwerke. Kleine Digitalfirmen sollen ebenfalls außen vor bleiben. Gemäß der Richtlinie müssen die Mitgliedstaaten nationale Meldesysteme aufbauen und Informationen untereinander austauschen. Beteiligt sind »kompetente Behörden« wie das BSI sowie spezielle Computersicherheits-Ereignis- und Reaktionsteams (Computer Security Incident Response Team, CSIRT). Der Rat der Europäischen Union möchte sie zusätzlich zu den bestehenden CERTs einrichten lassen. Den langen Verhandlungszeitraum von 2013 bis 2015 hat die Bundesregierung genutzt, um mit der Wirtschaft eine nationale Lösung zu erreichen, bevor sich die EU über das Thema einigte. Der Bundestag verabschiedete das IT-Sicherheitsgesetz im Juli 2015 und führte damit schon früher Meldepflichten bei schwerwiegenden Cyberangriffen und Mindeststandards für den Schutz kritischer Infrastrukturen ein.[76]

Enge Kooperation zwischen öffentlichen Stellen und privaten Unternehmen für die Sicherheit dieser Art von Infrastruktur ist allerdings nicht risikolos. Eine Selbstregulierung der Wirtschaft ist vor allem dann fragwürdig, wenn staatliche Akteure sich von den Interessen einzelner privater Akteure abhängig machen und ohne diese kaum in der Lage sind, sinnvoll zu handeln.[77] Diese Abhängigkeit wird umso prekärer, je stärker Unternehmen relevantes Wissen monopolisieren. Hier muss der Staat darauf achten, dass Parlamentarier und Vertreter der Zivilgesellschaft immer wieder Gelegenheit bekommen, kritisch nachzufragen, und in Konsultationsprozesse eingebunden werden.[78] Zur Sorgfaltsverantwortung gehört, dass nicht nur die Entscheidungen auf nationaler und europäischer Ebene, sondern auch die Entscheidungsvorbereitungsprozesse inklusiv und für die Belange der Zivilgesellschaft, der kleinen und mittleren Unternehmen und der unabhängigen Wissenschaft offen bleiben.

74 Ansgar Baums, »Der weiße Elefant: Industriepolitik durch die Hintertür des Datenschutzes?«, *plattform-maerkte.de*, 10.3.2015, <http://plattform-maerkte.de/der-weisse-elefant-industriepolitik-durch-die-hintertuer-des-datenschutzes/> (Zugriff am 30.11.2015).

75 Geschäftsstelle des UP KRITIS (Hg.), *UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen*, Bonn, Februar 2014, <www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.pdf?__blob=publicationFile> (Zugriff am 30.11.2015).

76 Ulrich Grillo, »Wege zur digitalen Republik«, in: *Handelsblatt*, 28.8.2015.

77 Annegret Bendiek, *Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein*, Berlin: Stiftung Wissenschaft und Politik, Juni 2013 (SWP-Aktuell 35/2013).

78 Bundesamt für Sicherheit in der Informationstechnik/Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, *Bund-Länder Kooperation*, <www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/BundLaender/bundlaender_node.html> (Zugriff am 5.2.2016); Bayerischer Landtag, *Schriftliche Anfrage des Abgeordneten Georg Rosenthal SPD vom 3.12.2014. Zur Sicherheit kritischer Infrastruktur in Bayern*, Drucksache 17/5186, München, 27.3.2015.

Zivilität

Es gilt der Versuchung zu widerstehen, auf die wachsende Zahl digitaler Angriffe mit dem Aufbau einer digitalen Rüstungsindustrie und damit Cyber-Offensivwaffen[79] zu reagieren. Die Verteidigungspolitischen Richtlinien des Bundesverteidigungsministeriums vom Mai 2011 enthalten bereits die Vorgabe, dass die deutschen Streitkräfte ein möglichst breites Fähigkeitsspektrum abdecken müssen.[80] Militärisch wird der Cyberraum als sogenannte operative Domäne qualifiziert, vergleichbar mit Land, Luft, See oder Weltraum. Laut der Strategischen Leitlinie Cyber-Verteidigung vom April 2015 soll es in Kampfeinsätzen möglich sein, »die Nutzung von Internet und Mobilfunk durch den Gegner einzuschränken, gegebenenfalls sogar auszuschalten«.[81] Derartige Formulierungen und Strategieentscheidungen bergen die Gefahr, dass der Cyberraum versicherheitlicht oder gar militarisiert wird und so eine neue Bedrohungskulisse entsteht.[82] Augenfällig wird diese Gefahr auf Konferenzen zur Cyber-Außen- und Sicherheitspolitik: Zwischen Herstellern von gepanzerten Fahrzeugen, ferngesteuerten Drohnen und Funkgeräten treffen Teilnehmer auf IT-Firmen wie McAfee, FireEye, Kaspersky, Symantec, Microsoft und einschlägige Startups, die hochspezialisierte Dienstleistungen anbieten. So ist es nicht verwunderlich, dass die private IT-Sicherheitsindustrie laut Schätzungen des Beratungsunternehmens Frost & Sullivan bis 2020 rund 155 Milliarden US-Dollar im Jahr umsetzen wird.[83] Hier entwickelt sich relativ eigenständig ein Markt, nämlich »Security as a service«[84], dessen Kehrseite »crime as a service« ist.

79 Eine offensive Waffe kann verstanden als »[a]n act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.« Nato, *Report on Cyber Defence Taxonomy and Definitions*, Enclosure 1 to 6200/TSC FCX 0010/TT-10589/Ser: NU 0289.

80 Bundesministerium der Verteidigung, *Verteidigungspolitische Richtlinien. Nationale Interessen wahren – Internationale Verantwortung übernehmen – Sicherheit gemeinsam gestalten*, Berlin, 27.5.2011.

81 Zitiert in Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), *FIfF fordert einen öffentlichen Diskurs über die neue Cyber-Sicherheitsstratgie der Bundeswehr*, Presseerklärung, Bremen, 15.7.2015.

82 James Andrew Lewis/Götz Neuneck, *The Cyber Index. International Security Trends and Realities*, New York/Genf: United Nations Institute for Disarmament Research (UNIDIR), 2013, <www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> (Zugriff am 30.11.2015).

83 Krzysztof Rutkowski, *Global Cyber Security Market Assessment. National Strategies Drive the Adoption of Cyber Solutions*, 17.2.2014, <www.frost.com/sublib/display-report.do?id=M875-01-00-00-00> (Zugriff am 30.11.2015).

84 »Security as a service« (SECaaS) als Sonderfall von »Software as a service« bedeutet Bereitstellung von IT-Sicherheitsdienstleistungen über das Internet und ist eine Form sicherheitskritischen IT-Outsourcings. Christian Senk, *Akzeptanz von Security-as-a-Service-Lösungen*, Berlin: Bitkom, 2011.

Cyberpolitiken im Zeichen der Sorgfaltsverantwortung

Die Norm der Sorgfaltsverantwortung besitzt direkte Relevanz für strategische Bereiche der deutschen Cyber-Außen- und Sicherheitspolitik. Deutschland, die EU und die Nato verfolgen bisher eine defensive Cybersicherheitsstrategie. Damit grenzt sich Deutschland auch von einzelnen EU- und Nato-Partnern wie Frankreich, Großbritannien, Niederlande und USA ab, die auf Abschreckung durch Drohung mit Vergeltung sowie auf Überwachungs- und Kontrolltechnologien setzen. Fatale Entscheidungen zu Vergeltung und Eskalation können die Folge sein, denn sie beruhen möglicherweise auf Fehlinterpretationen, weil Angreifer aus technischen, politischen und rechtlichen Gründen kaum zu identifizieren sind. Aus diesen Gründen wächst die Cyber-Unsicherheit in der internationalen Staatengemeinschaft. Staaten sind Nutzer von Informations- und Kommunikationstechnologien, müssen ihre Bürger und Daten schützen und gleichzeitig den digitalen Sektor regulieren, der weitestgehend von privaten Unternehmen dominiert wird. Zwar gilt es als ausgesprochen schwierig, durchgängig sichere Komponenten herzustellen, aber bei öffentlich eingesetzter Software kann auf Transparenz, Test und Analyse nicht verzichtet werden. Aus dieser Sachlage lässt sich ableiten, welche Bereiche einer Cyber-Außen- und Sicherheitspolitik am wichtigsten sind: Menschenrechts- und Datenschutzpolitik, Internet Governance, Cyberkriminalitätsbekämpfung, Cyberverteidigung und internationale Normenentwicklung. Alle fünf Bereiche überschneiden sich inhaltlich und konzeptionell. Das lässt schon erahnen, welche Probleme daraus erwachsen, etwa konfliktreiche Ressortabstimmung oder mangelnde Kohärenz und Inkonsistenzen in den Politiken, mit denen Herausforderungen im Cyberraum bewältigt werden sollen. Sorgfaltsverantwortung bedeutet in allen diesen Bereichen, die drei Anforderungen europäische Zusammenarbeit, Inklusivität und Zivilität zu beherzigen.[85]

85 Die Auswahl der folgenden Themenfelder einer Cyber-Außen- und Sicherheitspolitik erhebt keinen Anspruch auf Vollständigkeit. Die angeführten Beispiele dienen nur zur Illustration der hier genannten Anforderungen, die jede einzelne Politik im Sinne der Sorgfaltsverantwortung zu berücksichtigen hätte.

Menschenrechte und Datenschutz

Für liberale Demokratien sind Freiheitsrechte im Internet konstitutiv.[86] Spätestens seit den Enthüllungen des einstigen NSA-Mitarbeiters Edward Snowden 2013 zur staatlichen Ausspähpraxis ist jedoch klar, dass auch westliche Geheimdienste nicht nur passiv massenhafte Überwachung betreiben, sondern Computersysteme bewusst infiltrieren und kompromittieren. Organisationen wie Freedom House mit ihrer jährlichen Studie Freedom on the Net, Reporter ohne Grenzen oder Aktivisten für Freie Software weisen immer wieder darauf hin, dass Regierungen und global agierende IT-Konzerne weltweit keinen barrierefreien und kontinuierlichen Zugang zum Internet bereitstellen. Facebooks Projekt Internet.org etwa ermögliche lediglich den Zugang zu Facebook. Freiheitsaktivisten fordern, Internetzugang zum Menschenrecht zu erheben, doch die Debatte auf VN-Ebene zum Thema ist noch längst nicht entschieden.[87]

Der Menschenrechtsrat der VN betonte bereits im Juli 2012 in einer Resolution, dass Menschenrechte online wie offline in gleicher Form gültig sind.[88] Im Zuge einer deutsch-brasilianischen Initiative verabschiedete die VN-Generalversammlung im November 2013 eine Resolution zur Privatheit im digitalen Zeitalter, in der sie unter anderem die Massenüberwachung als illegal und undemokratisch ächtet.[89] David Kaye, VN-Sonderberichterstatter für Meinungsfreiheit, forderte im Mai 2015, die Verschlüsselung privater Kommunikation in der Breite zum Standard

86 Ben Wagner, »Freedom of Expression on the Internet: Implications for Foreign Policy«, in: *Global Information Society Watch*, 2011, S. 20–22.
87 Ben Wagner, »Könnt ihr mich hören?«, in: *Süddeutsche Zeitung*, 15.9.2015.
88 United Nations General Assembly, Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/20/L.13, New York, 29.6.2012, <www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc> (Zugriff am 9.12.2015).
89 United Nations General Assembly, *Third Committee Approves Text Titled »Right to Privacy in the Digital Age«, as It Takes Action on 18 Draft Resolutions*, GA/SHC/4094, New York, 26.11.2013, <www.un.org/press/en/2013/gashc4094.doc.htm> (Zugriff am 9.12.2015).

zu machen. Anfang Juli desselben Jahres schuf der VN-Menschenrechtsrat den Posten eines VN-Sonderberichterstatters zum Recht auf Privatheit und besetzte ihn mit dem Malteser Joseph Cannataci.[90] Allerdings reagieren Demokratien auf schwerwiegende Bedrohungen, etwa den islamistischen Terrorismus, bisweilen damit, dass sie den Ausnahmezustand ausrufen, wie die USA nach dem 11. September 2001 oder Frankreich nach den Terroranschlägen im November 2015 in Paris. Die »Reifeprüfung des Rechts«, so ein Kommentator, bestehe darin, während Ausnahmezuständen die Balance zwischen Freiheitsrechten und Sicherheitsmaßnahmen zu wahren.[91] Aufgabe des neuen Sonderberichterstatters ist es, zu dieser Balance in Bezug auf das Recht auf Privatheit Stellung zu beziehen.

Europäische Zusammenarbeit

Die europäische Erfahrung lehrt, dass integrierte Wirtschaftsräume längerfristig auch eine integrierte Innen- und Justizpolitik benötigen. Im Vertrag von Lissabon wird der Verwirklichung eines »Raums der Freiheit, der Sicherheit und des Rechts« große Bedeutung beigemessen. Die Grundrechte wurden gestärkt, indem gleichzeitig mit dem Lissabonner Vertrag 2009 eine für die EU rechtsverbindliche Charta der Grundrechte in Kraft trat und die EU verpflichtet wurde, der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten beizutreten. Was für den Binnenmarkt gilt, lässt sich auf den transatlantischen Wirtschaftsraum übertragen. Für den wirtschaftlichen Datentransfer haben sich EU und USA darauf geeinigt, einen sogenannten Schutzschirm für die Privatsphäre (Privacy Shield) auszuarbeiten. Verhandelt wird derzeit über ein transatlantisches Abkommen zum Datenschutz in der Strafverfolgung, das Schritte hin zur Harmonisierung von Straftatbeständen und zur wechselseitigen Weitergabe relevanter Daten und Informationen beinhalten könnte. Für die Bekämpfung der Cyberkriminalität ist eine intensive Kooperation von Strafverfolgungsbehörden zwingend. Die Online-Quellen der Finanzierung von Terrorismus, zum Beispiel digitale Finanzdienstleister, werden sich nur dann austrocknen lassen, wenn die USA und Europa bei der Umsetzung des Programms zum Aufspüren der Finanzierung des Terrorismus (Terrorist Finance Tracking Program, TFTP) und des Fluggastdatenaustauschs (Passenger Name Record, PNR) sowie bei der Weitergabe von Informationen eng zusammenarbeiten.[92] Terrorismusbekämpfung erfordert auch umfassende Geheimdienstkooperationen (wie etwa zwischen den »Five Eyes«[93]), die aber strenger parlamentarischer Kontrolle unterworfen werden müssen. Es ist nicht im Sinne der Sorgfaltsverantwortung, wenn Geheimdienste ihre Erkenntnisse informell austauschen und dabei die beispielsweise in Rechtshilfeabkommen[94] vorgesehenen rechtlichen Prozeduren unterlaufen.

90 Schon 2014 veröffentlichte die Hohe Kommissarin der Vereinten Nationen für Menschenrechte einen umfassenden Bericht zum Recht auf Privatsphäre im digitalen Zeitalter. United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, New York, 30.6.2014.

91 Andreas Zielcke, »Reifeprüfung des Rechts«, in: *Süddeutsche Zeitung*, 3.12.2015.

92 European Union, *Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program*, L 195/5, Brüssel, 27.7.2010; Council of the European Union, *Proposal for a Directive of the Council and the European Parliament on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*, 14670/15, Brüssel, 2.12.2015.

93 Dabei handelt es sich um die wichtigste Geheimdienstkooperation der anglophonen Welt, nämlich zwischen USA, Großbritannien, Kanada, Australien und Neuseeland. Siehe hierzu z.B. European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)* (2001/2098(INI), A5-0264/2001, Brüssel/Straßburg, 11.7.2001. Zur umfangreichen Geheimdienstkooperation im Kampf gegen transnationalen Terrorismus siehe Katarina Zivanovic, »International Cooperation of Intelligence Agencies against Transnational Terrorist Targets«, in: *PfP Consortium Quarterly Journal*, 8 (2008) 1, S. 115–141; Richard J. Aldrich, »International Intelligence Cooperation in Practice«, in: Hans Born/Ian Leigh/Aidan Wills (Hg.), *International Intelligence Cooperation and Accountability. Studies in Intelligence*, New York: Routledge, 2010, S. 18–41.

94 Rat der Europäischen Union, *Abkommen über Rechtshilfe mit den Vereinigten Staaten*, 2009/820/GASP, Brüssel, 23.10.2009; Deutscher Bundestag, *Gesetz zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Auslieferung, zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, zu dem Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen, zu dem Zweiten Zusatzvertrag vom 18. April 2006 zum Auslieferungsvertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika sowie zu dem Zusatzvertrag vom 18. April 2006 zum Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen (G-SIG: 16019368)*, Berlin, 26.10.2007.

Inklusivität

Je rechtsverbindlicher die Regulierungen zu Menschenrechten und Datenschutz sind, desto mehr steigen die Anforderungen an eine inklusiv gestaltete Rechtsumsetzung – so jedenfalls die europäische Erfahrung. In Deutschland und Europa ist der Datenschutz unmittelbar mit dem Recht auf informationelle Selbstbestimmung verknüpft. Dieses geht weit über die Norm der Sorgfaltsverantwortung hinaus, da der Staat gegenüber seinen Bürgern eine Schutzfunktion zu erfüllen hat. Fachlich zu unterscheiden sind der Datenschutz und die damit einhergehenden Schutzpflichten des Staates nach den Bereichen internationale Wirtschaftsverflechtung, Kriminalitätsbekämpfung und geheimdienstliche Zusammenarbeit. In jedem dieser Bereiche werden aufgrund ihrer Gefährdungen für die individuelle Freiheit und Sicherheit jeweils spezifische Vorkehrungen getroffen, die sich wiederum auf die Inklusivität von Regelungsbetroffenen auswirken.[95]

Der Datenschutz hat sich mittlerweile zur Rechtsmaterie einer geteilten Zuständigkeit in der EU entwickelt. Rechtsverbindliche Datenschutzbestimmungen zwischen Staaten wurden bislang nur im regionalen Maßstab beschlossen, nämlich 1981 in Form der Datenschutzkonvention des Europarates. Im Trilog zwischen Vertretern der Kommission, des Europäischen Parlaments und des Rats der EU einigte man sich im Dezember 2015 auf ein Reformpaket zum Datenschutz in Gestalt der Datenschutzgrundverordnung (DSGVO[96]), welche die EU-Datenschutzrichtlinie von 1995 abgelöst hat. Die neue Verordnung wird ab 2018 direkt in nationales Recht umzusetzen sein. Zum Reformpaket der DSGVO gehört die Richtlinie, die einen harmonisierten Rechtsrahmen für Regeln zur Datenverarbeitung in Polizei- und Justizbehörden der EU-Länder vorsieht. Gemäß DSGVO ist es in Zukunft untersagt, zu kommerziellen und anderen Zwecken in der EU erhobene Daten an Gerichte oder Behörden von Drittstaaten weiterzugeben. Die bekanntesten Beispiele für eine solche Praxis sind die großen Anbieter digitaler Dienstleistungen wie Amazon, Google und Facebook, die Daten von europäischen Kunden in den USA speichern und hierbei Datenschutzbestimmungen anwenden, die europäischem Recht widersprechen. Bei schwerwiegenden Verstößen gegen das Datenschutzrecht können Datenschutzbehörden künftig drastische Strafzahlungen über Unternehmen verhängen. Diese Behörden spielen als Beschwerde- und Kontrollstellen eine immer wichtigere Rolle, denn sie prüfen, wie mit personenbezogenen Daten umgegangen wird, und können Sanktionen veranlassen.[97] Deshalb sollte ihre Unabhängigkeit gestärkt und der Einfluss privatwirtschaftlicher Unternehmen auf sie begrenzt werden. Der EuGH hat in zwei Urteilen (2010 und 2012) klargestellt, dass Datenschutzbeauftragte und ihre Behörden »völlige Unabhängigkeit« genießen müssen.[98]

95 Neben den entsprechenden Rechtssätzen im Grundgesetz sind die rechtlichen Grundlagen im primären Geheimdienstrecht und im Recht der Polizeien und sonstigen Behörden geregelt: Bundesdatenschutzgesetz (BDSG), Telekommunikationsgesetz (TKG), Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10), Gesetz über das Bundeskriminalamt (BKAG), Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG), Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz – ZFdG), Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG), Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG), Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz – MADG), Verordnung über die Übermittlung von Auskünften an die Nachrichtendienste des Bundes (Nachrichtendienste-Übermittlungsverordnung – NDÜV).

96 Rat der Europäischen Union, *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Drucksache 5455/16, Brüssel, 28.1.2016.

97 Der bzw. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit soll Telekommunikations- und Postdienstleister, Bundesbehörden und andere öffentliche Stellen des Bundes beim Datenschutz kontrollieren. Anders als seine bzw. ihre Amtskollegen in den Ländern kann er bzw. sie bei Verstößen nur Ermahnungen aussprechen, aber keine Bußgelder verhängen.

98 Europäischer Gerichtshof, Urteil des Gerichtshofs (Große Kammer), *Vertragsverletzung eines Mitgliedstaats – Richtlinie 95/46/EG – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und freier Datenverkehr – Art. 28 Abs. 1 – Nationale Kontrollstellen – Unabhängigkeit – Behördliche Aufsicht über diese Stellen*, Rechtssache C-518/07, Luxemburg, 9.3.2010; Europäischer Gerichtshof, Urteil des Gerichtshofs (Große Kammer). *Vertragsverletzung eines Mitgliedstaats – Richtlinie 95/46/EG – Verarbeitung personenbezogener Daten und freier Datenverkehr – Schutz natürlicher Personen – Art. 28 Abs. 1 – Nationale Kontrollstelle – Unabhängigkeit – Kontrollstelle und Bundeskanzleramt – Persönliche und organisatorische Bindungen*, Rechtssache C-614/10, Luxemburg, 16.10.2012.

Zivilität

Die zur Strafverfolgung notwendigen Daten werden nicht allein durch IT-Techniken im jeweiligen Land generiert. Der betreffende EU-Mitgliedstaat wird immer auch auf Datenquellen zurückgreifen, die in verbündeten Staaten unter anderen rechtlichen Voraussetzungen zustande kamen und den hohen deutschen und europäischen Ansprüchen an Datenschutz nicht genügen. Eine verstärkte Vorratsdatenspeicherung, um die polizeiliche Arbeit zu unterstützen, wird zwar als wichtiges Instrument bei der Kriminalitätsbekämpfung im Cyberraum gesehen. Auskunft über in der Vergangenheit angefallene Verkehrsdaten und deren Erhebung sind aber seit dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 unzulässig. Am 8. April 2014 verwarf der EuGH auch die EU-Richtlinie zur Vorratsdatenspeicherung, weil sie mit der Charta der Grundrechte der EU unvereinbar sei. Der von Bundesjustizminister Heiko Maas 2015 vorgelegte Gesetzesentwurf sieht nun vor, Telekommunikationsdaten aller Bürger zehn Wochen lang zu speichern. Für die Standortdaten, die bei der Handynutzung anfallen, soll eine verkürzte Speicherfrist von vier Wochen gelten.[99] Inwieweit der neue Entwurf mit den Grundrechten in Einklang steht, bleibt abzuwarten. Technisch ist dieses Instrument derweil fast überholt.

Jedenfalls zeichnet sich ab, dass Big Data[100] auch für die Strafverfolgung immer interessanter wird.[101] Verwendet werden dazu vorhandene Datenquellen, Algorithmen und vorausschauende Analysen (Predictive Analytics).[102] Eine weitere Methode ist die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Damit reagieren die Behörden auf die zunehmende Verschlüsselung der Kommunikation[103] auf Bundesebene.[104] Ermittlungsbehörden installieren dabei ein auch »Bundestrojaner« genanntes Programm auf dem Computer eines Verdächtigen.[105] Damit können E-Mails, Internet-Telefonie oder Chats direkt am System mitgeschnitten und weitergeleitet werden, bevor die Kommunikation vom Programm verschlüsselt wird. Der Bundestrojaner ist umstritten, weil er auch als Cyberwaffe eingestuft werden kann, deren Anwendung dann parlamentarisch abgesichert werden müsste. Um den Sachverhalt besser beurteilen und einordnen zu können, wäre möglicherweise mehr Zusammenarbeit zwischen Behörden und Wissenschaft hilfreich. Im Bereich der Prävention hat die Bundesregierung im März 2015 ein ressortübergreifendes Forschungsprogramm für mehr Sicherheit im Internet gestartet. Seine Schwerpunkte lauten (1) Neue Technologien, (2) Sicherheit und vertrauenswürdige Informations- und Kommunikationssysteme, (3) Anwendungsfelder der Sicherheit sowie (4) Privatheit und Schutz von Daten. Das Bundesbildungsministerium wird das Programm unter dem Titel »Sicher und selbstbestimmt in der digitalen Welt« bis zum Jahr 2020 mit insgesamt etwa 180 Millionen Euro fördern.[106]

99 Nicht davon erfasst sind Abhörmaßnahmen der Polizei zu präventiven Zwecken und die nicht von der Justiz kontrollierten Eingriffe der Nachrichtendienste in das Fernmeldegeheimnis. Für den präventiv-polizeilichen Bereich gilt das BKA-Gesetz vom 25. Dezember 2008. Gerd Lehmann, »Wie geht es jetzt – wie in Zukunft?«, in: *Behörden Spiegel*, Juli 2015.

100 Der Begriff Big Data beschreibt die automatisierte, computergestützte Verarbeitung großer heterogener Datenmengen. Sie birgt große Potentiale insbesondere für Wirtschaft und empirische Wissenschaften. Bundesministerium für Bildung und Forschung, *Big Data – Management und Analyse großer Datenmengen*, <www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html> (Zugriff am 5.2.2016).

101 Ein Beispiel hierfür ist die Software Child Abuse Prevention System (CAPS), die vom Diplomatic Council betrieben wird, einem globalen Think Tank mit besonderem Beraterstatus bei den VN. CAPS ergänzt vorhandene Infrastrukturen, Prozesse und Lösungen der Strafverfolgungsbehörden weltweit und unterstützt das Bündnis White IT, das Kinderpornografie bekämpft. Als problematische Nebenwirkungen neuer Strafverfolgungstechniken gelten Massenüberwachung, ungerechtfertigter Generalverdacht sowie die Verlagerung von Ressourcen weg von personeller Ausstattung und hin zu technischen Lösungen. James Byrne/Gary Marx, »Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact«, in: *Cahiers Politiestudies*, 3 (2011) 20, S. 17– 40 (32).

102 Walter L. Perry/Brian McInnis/Carter C. Price/Susan C. Smith/John S. Hollywood, *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation, 2013.

103 Siehe hierzu Sandvine (Hg.), *Global Internet Phenomena Spotlight. Encrypted Internet Traffic*, Waterloo, Ontario, 2015, <www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf> (Zugriff am 5.2.2016).

104 Mit der Digitalen Agenda 2014–2017 setzte sich die Bundesregierung das Ziel, »Sicherheit und Schutz im Netz« herzustellen. Sie kündigte sogar an, »Verschlüsselungs-Standort Nr. 1 auf der Welt« zu werden.

105 Deutscher Bundestag, *Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, Petra Pau, Jens Petermann, Frank Tempel, Halina Wawzyniak und der Fraktion Die Linke. Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage (»Staatstrojaner«)*, Drucksache 17/7104, Berlin, 25.10.2011.

106 Bundesministerium für Bildung und Forschung (Hg.), *Selbstbestimmt und sicher in der digitalen Welt 2015–2020. For-*

Internet Governance

In der Internet Governance geht es darum, sich auf technische Standards und Regeln für die grenzüberschreitende Verknüpfung nationaler Netze zu einigen.[107] Wesentliche Herausforderungen hierbei liegen darin, Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität von Daten zu gewährleisten. Mit der Digitalen Agenda 2014–2017[108] unterstützt die Bundesregierung die Fortführung des Multistakeholder-Ansatzes der Internet Governance. Zur Neuausrichtung der Internet-Verwaltung[109] ist Deutschlands Vorgehen mit den anderen europäischen Staaten abzustimmen. Schwachstellen in Hard- und Softwareprodukten sowie Fragen der Kryptologie sind ebenfalls zu diskutieren. In der Internet Governance sollen die Stakeholder – private Nutzer, Zivilgesellschaft, Wissenschaft, Unternehmen, Regierungen – in ihrer jeweiligen Rolle verantwortlich handeln und an der Entwicklung des Internets beteiligt werden. Auf diese Weise soll dafür Sorge getragen werden, dass breit legitimierte Entscheidungen gefällt werden. Wichtige Komponenten eines funktionierenden und verlässlichen Internet-Governance-Systems sind internationale Organisationen und Foren wie die Internet Corporation for Assigned Names and Numbers (ICANN), die für das stabile Funktionieren des Internets zuständig ist, die Information Society (ISOC), die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und das in der Folge des Weltgipfels zur Informationsgesellschaft der VN etablierte Internet Governance Forum (IGF), das Multistakeholder-Forum auf globaler Ebene mit 3700 Mitgliedern aus 144 Ländern.[110] Staaten sollen nur dort regulierend eingreifen, wo demokratische Legitimität, Effektivität, Rechtsstaatlichkeit und Transparenz nicht durch Selbstregulierung sichergestellt werden können. Multilaterale Zusammenarbeit kommt dort ins Spiel, wo Belange von Staaten mit weniger ausgeprägten Internetkapazitäten in die Internet Governance einbezogen werden sollen. In Deutschland wird das Bundesministerium für Wirtschaft und Energie die Zukunft der Internet Governance und Industrie 4.0 federführend gestalten.[111] Aus der Norm der Sorgfaltsverantwortung lässt sich die Notwendigkeit einer Reihe von Reformen der Internet Governance ableiten:

Europäische Zusammenarbeit

Die Bundesregierung sollte ihre nationale Position mit den EU-Partnern und anderen Staaten insbesondere der OECD abstimmen, um die Voraussetzungen zu schaffen, in den Vereinten Nationen (wie zuletzt auf der WSIS-Folgekonferenz im Dezember 2015) ihre Auffassungen international durchzusetzen. Alleingänge sind schon deswegen zwecklos, weil Deutschlands Verhandlungsmacht in den multilateralen Foren, aber auch denen der Internet Governance zu gering ist. Im Juni 2011 wurde die Position der EU festgelegt, indem die Europäische Kommission erklärte, angestrebt werde die Schaffung eines »einzigen, offenen, freien und unfragmentierten Netzwerkes von Netzwerken, welches denselben Gesetzen und Normen unterliegt, die in anderen Bereichen unseres täglichen Lebens vorherrschen«.[112] Die EU wie auch Deutschland unterstützen eine führende Rolle des Internet Governance Forum, dessen Laufzeit auf dem VN-Gipfel im Dezember 2015 um weitere fünf Jahre verlängert wurde. So sollen intergouvernementale Einflussnahme zuungunsten des Multistakeholder-Ansatzes verhindert sowie Organe und Funktionen wie ICANN und IANA (Internet Assigned Numbers Authority) »internationalisiert« werden. Darunter versteht die EU einen inklusiven Dialog mit Entwicklungs-, Schwellen- und Industrieländern im Sinne innovativer »best practices« mit dem Ziel, den Internetzugang auch im ländlichen Raum sicherzustellen (Capacity Building). Mit Hilfe der Internet Governance soll die Informations- und Kommunikationstechnologie auch in weniger ent-

schungsrahmenprogramm der Bundesregierung zur IT-Sicherheit, Bonn/Berlin 2015.

107 Deutscher Bundestag, *Aktueller Begriff. Internet Governance*, Drucksache 11/14, Berlin, 27.3.2014. Zur Diskussion über Nutzung und Weiterentwicklung des Internets wird das Internet-Modell zugrunde gelegt, das Netzzonen des Internets und technische Ebenen der Kommunikation kombiniert.

108 BMWi/BMI/BMVI, *Digitale Agenda 2014–2017* [wie Fn. 65].

109 Internet Society, *IANA Transition*, <www.internetsociety.org/ianaxfer> (Zugriff am 5.2.2016).

110 Stand 2014. Siehe Website des IGF, <www.intgovforum.org/cms/> (Zugriff am 5.2.2016).

111 Bundesministerium für Wirtschaft und Energie (Hg.), *Industrie 4.0 und Digitale Wirtschaft. Impulse für Wachstum, Beschäftigung und Innovation*, Berlin, April 2015.

112 Das einschlägige Akronym hierfür lautet COMPACT (*C*ivic Responsibilities, *O*ne Unfragmented Resource, *M*ultistakeholder Approach to *P*romote Democracy and Human Rights, Sound Technological *A*rchitecture, *C*onfidence and *T*ransparent Governance). European Commission, *Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance*, COM(2014) 72 final, Brüssel, 12.2.2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072&from=EN> (Zugriff am 30.11.2015).

wickelten (Welt-)Regionen kontinuierlich verbessert werden.

Inklusivität

In der globalen Internet Governance sind Inklusivität und Legitimität hoch umstritten.[113] An der Setzung globaler Internetstandards sollten aber zivilgesellschaftliche Interessengruppen und Parlamentarier beteiligt sein, damit nicht nur technische Gremien wie das Internet Architecture Board die Entscheidungen treffen. Nur durch Inklusivität lässt sich gewährleisten, dass die nötige Fachkompetenz bereitgestellt und gesellschaftliche Akzeptanz für Standardsetzungsprozesse erzeugt wird. Darüber hinaus sollen die IANA-Funktionen bei der Vergabe von Top-Level-Domains, also der höchsten Ebene von Namensauflösungen wie etwa »*.com« oder »*.de«, auf eine allseits akzeptable Basis gestellt werden. Der Multistakeholder-Prozess in der Internet Governance konnte um weitere fünf Jahre verlängert werden, denn die VN-Generalversammlung beschloss Ende 2015, dass das IGF seine Tätigkeit fortsetzen soll.[114] Nicht verhindern ließ sich, dass Sicherheitsbelange einzelner Regierungen wie Russlands oder Saudi-Arabiens auch in Fragen der Internet-Verwaltung eine immer größere Rolle spielen.[115]

Zivilität

Voraussetzungen für die Zivilisierung digitaler Kommunikation sind Vertraulichkeit, Integrität und Verlässlichkeit. Kommunikation findet in einem globalen Netzwerk aus Netzwerken statt, dessen Server auf der ganzen Welt verteilt sind. Der Standort dieser Server hat daher nur wenig Einfluss auf Sicherheit und Privatheit der Kommunikation. Weitaus wichtiger sind etablierte Zertifizierungsstandards. Nutzer können E-Mails verschlüsseln, Einmal-Adressen[116] anlegen oder auf die De-Mail[117] bauen. Gleichwohl reklamieren Staaten für sich das Recht, bei der Strafverfolgung auf verschlüsselte Kommunikation zurückzugreifen und zu diesem Zweck »Hintertüren«[118] in die Systeme von Verdächtigen einzubauen. Auch gut verschlüsselte E-Mails hinterlassen Metadaten, die viele Auskünfte über Absender, Empfänger, Betreffe und Zeit geben. Geheimdienste wie die NSA sammeln solche Daten in großem Stil. Um dies zu erschweren, wird intensiv an Verschlüsselungstechniken gearbeitet.[119] Bei der Zivilisierung der Kommunikation spielen die Nutzer selbst eine entscheidende Rolle. Sie können Druck aufbauen, damit sich eine anwenderfreundliche, anspruchsvolle und ausdifferenzierte Verschlüsselung durchsetzen lässt. Deshalb liegt es zwar nahe, Cybersicherheit auch in den Gremien der Internet Governance immer häufiger zum Thema zu machen. Abzuraten ist jedoch von einer Versicherheitlichung der Internet-Verwaltung und wachsendem staatlichem Einfluss auf sie, mit der Ausnahme, dass staatliche Organe hier ihrer Sorgfaltsverantwortung nachkommen wollen. Grundsätzlich bleibt die Internet Governance aber bis auf Weiteres in den Händen privater Akteure.

Cyberkriminalitätsbekämpfung

Die Bekämpfung der Cyberkriminalität umfasst alle nichtmilitärischen Maßnahmen, die dem Schutz

113 Annegret Bendiek/Christoph Berlich/Tobias Metzger, *Die digitale Selbstbehauptung der EU*, Berlin: Stiftung Wissenschaft und Politik, August 2015 (SWP-Aktuell 71/2015), S. 6f.
114 United Nations General Assembly, *Outcome Document of the High-level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society*, A/70/L.33, New York, 13.12.2015.
115 Monika Ermert, »WSIS+10: Zehn Jahre nach dem großen Gipfel«, *heise online*, 14.12.2015, <www.heise.de/newsticker/meldung/WSIS-10-Zehn-Jahre-nach-dem-grossen-Gipfel-3043792.html> (Zugriff am 5.2.2016).
116 Provisorische E-Mails werden auch unter den Bezeichnungen Wegwerf-E-Mail oder Instant E-Mail angeboten. Sie sollen den Verlust persönlicher Daten möglichst begrenzen, wenn Integritätsverluste, also Informationsverfälschungen, bei Websitebetreibern auftreten.
117 In Form des De-Mail-Gesetz (De-Mail-G, 28.4.2011) setzte die Bundesregierung die europäische Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt um. Mit De-Mail können Nachrichten und Dokumente über das Internet vertraulich, sicher und nachweisbar versendet und empfangen werden. Sie wird von verschiedenen E-Mail-Dienstleistern in Deutschland angeboten und kann u.a. für den digitalen Briefverkehr mit vielen Ministerien genutzt werden. *E-Mail made in Germany. Eine Initiative von GMX, Telekom und WEB.DE*, <www.e-mail-made-in-germany.de/index.html> (Zugriff am 5.2.2015).
118 Als Backdoors werden bewusst platzierte Schwachstellen in Hard- und Software bezeichnet, die es ermöglichen, zu einem späteren Zeitpunkt auf bestimmte Funktionen der betreffenden Computer oder Programme zuzugreifen.
119 Siehe z.B. Johannes Wendt, »Wie Dark Mail die Metadaten abschaffen will«, in: *Zeit Online*, 7.1.2015, <www.zeit.de/digital/datenschutz/2015-01/darkmail-verschluesselung-metadaten-email-lavabit> (Zugriff am 30.11.2015).

ziviler Ziele vor digitalen Angreifern dienen. In erster Linie geht es um kritische Infrastrukturen und persönliche (Freiheits-)Rechte. Seit den Anschlägen des 11. September 2001 haben die Vereinten Nationen zur Terrorismusbekämpfung zahlreiche Resolutionen beschlossen, die auch Ausgangspunkte für die Cybersicherheit bilden können. Deutschland hat die Budapester Konvention des Europarates[120] zur Cyberkriminalitätsbekämpfung ratifiziert und unterstützt die EU-Cybersicherheitsstrategie vom Februar 2013[121], mit der die Union den gleichen Ansatz wie Deutschland verfolgt, nämlich eine defensive und polizeiliche Ausrichtung der Cyber-Sicherheitspolitik. Bisher beschränkt sie sich auf eine koordinierende Rolle bei dem Bestreben, einen »offenen, sicheren und geschützten Cyberraum« zu erreichen. Schwerpunkte dabei sind a) die Schaffung resilienter IKT-Strukturen, b) der Kampf gegen Cyberkriminalität, c) die Entwicklung von Cyberverteidigungsfähigkeiten, d) die Förderung industrieller und technologischer Entwicklungen zur Cybersicherheit sowie e) die Entwicklung einer internationalen Cyberdiplomatie.[122] Erfolge und Perspektiven der Inneren Sicherheit in Europa hängen davon ab, dass sie auf nationaler, europäischer und internationaler Ebene ansetzt, dabei die technischen Möglichkeiten des Informationsaustauschs zwischen den Ebenen nutzt und diesen rechtlich absichert. Globalisierung, Automatisierung und Industrialisierung von Kriminalität setzen internationale und europäische Zusammenarbeit voraus, insbesondere eine strukturelle Vernetzung auch auf den Arbeitsebenen der Strafverfolgungsbehörden.[123]

Europäische Zusammenarbeit

Um der Sorgfaltsverantwortung beim Kampf gegen Cyberkriminalität Geltung zu verschaffen, muss das materielle Strafrecht dringend harmonisiert werden, vor allem die Definition von Straftatbeständen. Zwar haben die meisten Mitgliedstaaten der EU die Budapester Konvention unterzeichnet und sich damit verpflichtet, Delikte im Cyberraum strafrechtlich zu verfolgen. Weit auseinander gehen allerdings die rechtlichen Auffassungen der EU-Länder darüber, welche Handlungen im digitalen Bereich überhaupt als Straftaten zu bewerten sind und inwieweit sie geahndet werden sollen. Es wäre nicht zweckmäßig, Straftatbestände mit Hilfe intergouvernementaler Vereinbarungen oder einzelstaatlicher Regelungen zu harmonisieren. Gefragt ist vielmehr ein Verfahren, das alle EU-Staaten einbezieht und sich am ordentlichen Rechtsetzungsprozess der Union orientiert. Noch aber besitzt diese keine Kompetenzen für die Harmonisierung des Strafrechts. Ihr derzeitiges rechtliches und politisches System fußt immer noch darauf, dass es innerhalb nationalstaatlicher Grenzen gilt und wirkt. Zugleich wird es aber schwieriger, Zugriffsbefugnisse rechtlich einzuordnen, da beispielsweise Cloud-Dienste über Kontinente hinweg operieren. Dennoch sollte die EU sich bei der Herstellung vernetzter Sicherheit auf die Strafverfolgung konzentrieren. Sinnvoll sind Initiativen wie der Europäische Haftbefehl, die Einrichtung einer Europäischen Staatsanwaltschaft oder die Richtlinie über die Verwendung von Fluggastdatensätzen einschließlich entsprechender transatlantischer Abkommen. Um Unternehmen den Anreiz zu nehmen, ihre Geschäfte ins Ausland zu verlagern und auf diese Weise die Sorgfaltsverantwortung zu umgehen, wären die Vorgaben zur Datensicherheit auf EU-Ebene (NIS-Richtlinie) mit denjenigen des National Institute of Standards (NIST) der USA in Einklang zu bringen. Transatlantische Zusammenarbeit spielt nicht nur in öffentlich-privaten Partnerschaften eine wichtige Rolle, sondern auch auf offizieller Ebene, hier in der EU-USA-Arbeitsgruppe zur Cyberkriminalitätsbekämpfung.[124]

Inklusivität

Sicherheitsbehörden auf EU- und nationalstaatlicher Ebene werden sich darauf einstellen müssen, dass auf die Mitarbeit privater Akteure beim Kampf gegen Cyberkriminalität nicht mehr verzichtet werden kann. Eine klare Trennung zwischen privat und öffentlich

120 Europarat, *Übereinkommen über Computerkriminalität*, SEV Nr. 185, Budapest, 23.11.2001.

121 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, Brüssel, 7.2.2013.

122 Ebd., S. 4f.

123 »Digitale Agenda«, Interview mit dem niedersächsischen Innenminister Boris Pistorius, in: *Behörden Spiegel*, Februar 2014.

124 Annegret Bendiek, *Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit*, Berlin: Stiftung Wissenschaft und Politik, Dezember 2013 (SWP-Studie 26/2013); European Parliament, Directorate-General for Internal Policies, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Study for the LIBE Committee*, Brüssel 2015.

lässt sich in diesem Bereich kaum mehr aufrechterhalten, denn oft verfügen nur die angegriffenen Unternehmen über Möglichkeiten, Cyberangriffe aufzuklären. Konzerne wie Microsoft lassen sich sogar per Gerichtsbeschluss zu sogenannten Hackbacks ermächtigen, also dazu, ihrerseits in IT-Systeme der Angreifer einzudringen, etwa um Gruppen automatisierter Schadprogramme, sogenannte Botnetze, zu zerschlagen.[125] Zwar ist es weiterhin schwierig, Cyberattacken zweifelsfrei zuzuordnen, beispielsweise aufgrund gefälschter Abrechnungen, Sabotage von Computersystemen und Passwortdiebstahl. Dennoch hinterlassen Täter digitale Spuren. Dreh- und Angelpunkt der Strafverfolgung ist darum das Rekonstruieren und Analysieren, die IT-Forensik.[126] Die deutschen Behörden, darunter das BKA und die Landeskriminalämter, unterstützen deshalb den Aktionsplan des Europäischen Polizeiamts (Europol).[127] Mittlerweile suchen Strafverfolgungsbehörden auch gezielt nach Gefahren im IT-System (Threat Hunting), statt nur auf Attacken zu reagieren. Bei Erfolg ist es möglich, Angreifern den Zugang zu den sensibelsten Bereichen zu versperren. Voraussetzung ist aber eine softwaregestützte, gerichtsfeste Konservierung digitaler Daten. Die Beweismittelsicherung bei großen und komplexen Datenbeständen ist langwierig und benötigt äußerst leistungsfähige Computer. Digitale Forensik sieht sich also vor immense Herausforderungen gestellt. Bei der Aufklärung von Straftaten setzen Behörden daher auch auf die Unterstützung durch private IT-Forensiker. Aber die öffentlich-privaten Sicherheitskooperationen zeigen Schwächen, auch weil die Selbstvernetzung der Wirtschaft in der Kriminalitätsabwehr bisher nicht sehr ausgeprägt ist, abgesehen von der BSI-Initiative Allianz für Cyber-Sicherheit und von CERT-Austauschen. Schon seit 2006 existiert die Global-Player-Initiative, ein Netzwerk, an dem das BKA und zurzeit 62 Großunternehmen beteiligt sind. Insgesamt kooperiert das BKA mit rund 630 Betrieben. Oft verläuft der Informationsaustausch indes noch als eine Art Einbahnstraße, weil vor allem kleine und mittelständische Unternehmen nicht über genug Kapazitäten verfügen, um weitreichende IT-Sicherheitsmaßnahmen zu ergreifen. In Deutschland sind Betreiber kritischer Infrastrukturen durch das IT-Sicherheitsgesetz dazu verpflichtet, Cyberattacken zu melden und IT-Mindestsicherheitsstandards einzuführen. Unzureichend geklärt sind bislang Sicherheitsfragen bei Softwareprodukten und externen Cloud-Services. Intensiv diskutiert werden derzeit verpflichtende Sicherheitstests sowie eine Ausweitung der Herstellerhaftung.[128]

Zivilität

Gemäß der EU-Cybersicherheitsstrategie soll Kriminalität im Cyberraum ausschließlich mit nichtmilitärischen Mitteln bekämpft werden. Um den vorrangigen Interessen der EU dabei Rechnung zu tragen, wäre es notwendig, den relevanten Stellen mehr supranationale Kompetenzen und finanzielle Mittel zu gewähren. Dazu zählen das European Cybercrime Center (EC3) bei Europol[129], die Europäische Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency, ENISA) und die Justizbehörde der Europäischen Union (European Union's Judicial Cooperation Unit, Eurojust). Unspektakulär, aber im Sinne der Sorgfaltsverantwortung wichtig für den Aufbau resilienter IKT-Strukturen sind Cyberübungen, die regelmäßig auf nationaler, aber auch auf EU-Ebene von der ENISA koordiniert werden. An der Übung Cyber Europe 2014 waren 29 EU-EFTA-Staaten sowie 200 internationale Regierungsorganisationen beteiligt.[130] Dabei sollte getestet werden, wie sich die zwischenstaatliche Kooperation bei der Bewältigung von Cyber-Sicherheitsvorfällen in ganz Europa verbessern ließe, wie sich die zahlreichen parallelen Kommunikationsbeziehungen auf die Erstellung eines nationalen und eines europäischen Lagebildes auswirken und welche Folgen eine übergreifende europäische Cyberkrise auf Presse- und Öffentlichkeitsarbeit der Teilnehmerstaaten hätte. Auf der operativen Ebene ist es unabdingbar, dass die IT-Notfallteams kontinuierlich mit anderen CERTs zusammenarbeiten. So ist das BSI Mitglied in der European Government

125 Janine S. Hiller, »Civil Cyberconflict: Microsoft, Cybercrime, and Botnets«, in: *Santa Clara High Technology Law Journal*, 31 (2015) 2, S. 163–214.

126 Bundesamt für Sicherheit in der Informationstechnik, *Leitfaden »IT-Forensik«*, Version 1.0.1, Bonn, März 2011.

127 Deutscher Bundestag, *Antwort auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion Die Linke, Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen mit deutscher Beteiligung*, Drucksache 18/4585, Berlin, 10.4.2015.

128 Bundesamt für Sicherheit in der Informationstechnik (Hg.), *Die Lage der IT-Sicherheit in Deutschland 2015* [wie Fn. 27].

129 Europol, *European Cybercrime Center (EC3)*, <www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837> (Zugriff am 5.2.2016).

130 European Network and Information Security Agency, *ENISA CE2014. After Action Report*, Heraklion 2014.

CERTs Group (EGC), einer informellen Gruppe auf europäischer Ebene, und im Forum for Incident Response and Security Teams (FIRST), einem internationalen Zusammenschluss von rund 200 staatlichen und privaten CERTs.[131]

Cyberverteidigung

Das Nato-Zentrum für die Abwehr von Cyberangriffen (Cooperative Cyber Defence Centre of Excellence, CCDCOE) wird von elf Mitgliedstaaten des Bündnisses finanziert, ist aber nicht Teil von dessen Kommandostruktur. Mit dem Tallinn Manual 2013, an dem auch deutsche Wissenschaftler mitarbeiteten, hat das Zentrum Vorschläge unterbreitet, das Recht zum Krieg (ius ad bellum) und das Recht im Krieg (ius in bello) für den Cyberraum zu kodifizieren.[132] Dabei haben die Autoren auch zu formulieren versucht, wie Sorgfaltspflichten im Cyberraum Genüge getan werden könnte. So heißt es im Tallinn Manual: »(a) State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.«

Gemäß ihrem Verfassungsauftrag innerhalb der Bündnisverteidigung verfügt auch die Bundeswehr in erster Linie über defensive Cyberfähigkeiten, ist also auf digitale Verteidigung ausgerichtet.[133] Diese umfasst Maßnahmen zur Abwehr von Bedrohungen nicht nur einzelner Personen oder Unternehmen, sondern des Staates und seiner gesellschaftlichen Grundlagen. Die Bundeswehr sieht sich auch im Cyberraum als zentrale Instanz zur Abwehr äußerer Gefahren. Zur Cyberverteidigung gehören laut der deutschen Sicherheitsstrategie die militärisch genutzten IT-Systeme und der deutsche Anteil am Cyberraum. Seit einiger Zeit ist nicht nur zu beobachten, dass immer häufiger digitale Konflikte im Cyberraum ausgetragen werden, sondern auch, dass militärische Einsätze unterhalb der Schwelle des bewaffneten Konflikts stattfinden, an denen nichtstaatliche Akteure beteiligt sind. Deswegen weist die Bundesregierung ausdrücklich darauf hin, dass auch militärische Akteure für digitale Angriffe verantwortlich sein können.

Europäische Zusammenarbeit

In der Cyberverteidigungspolitik sollte frühzeitig auf europäische und atlantische Kooperation gedrängt werden, immer mit dem Ziel, die Leitidee der Sorgfaltsverantwortung durchzusetzen. Nationale Maßnahmen, mit denen die Qualität eingesetzter Komponenten und Schlüsseltechnologien geprüft und gesteigert wird, sollten sich auf die Aufklärung und den Informationsaustausch in der EU sowie zwischen EU und Nato stützen. Der Europäische Rat hat im Dezember 2013 angekündigt, die Zusammenarbeit zwischen EU und Nato zu intensivieren, und im November 2014 ein Rahmenkonzept zur Cyberverteidigung (Cyber Defence Policy Framework) verabschiedet.[134] Damit sollen der Schutz von Missionen in der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) und die Kommunikationssicherheit des Europäischen Auswärtigen Diensts (EAD) erhöht werden.[135]

In ihrem Strategischen Konzept aus dem Jahr 2010 erklärte die Nato, dass Cyberangriffe den »nationalen und euro-atlantischen Wohlstand, Sicherheit und Stabilität gefährden können«.[136] Als Konsequenz daraus beschloss die Allianz im Juni 2014 bei ihrem Gipfel in Wales eine verbesserte defensive Cyberverteidigungspolitik (Nato Enhanced Cyber Defence Policy) mit dem Ziel, resiliente Strukturen aufzubauen.[137] Neben Konsultations- und Unterstützungsprozessen gibt es auch gemeinsame Übungen, etwa dazu, wie Cyberangriffen begegnet werden kann. So organisiert die

131 European Government CERTs Group, *Members of the European Government CERTs Group*, <www.egc-group.org/contact.html> (Zugriff am 30.11.2015); Forum for Incident Response and Security Teams, *FIRST Members*, <www.first.org/members> (Zugriff am 30.11.2015).
132 Schmitt (Hg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* [wie Fn. 9].
133 Bundesministerium der Verteidigung, *Von der Leyen reformiert Cyber-Strukturen*, Berlin, 17.9.2015.
134 Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, Brüssel, 18.11.2014, <www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf> (Zugriff am 3.12.2015).
135 European External Action Service, *EU International Cyberspace Policy*, <http://eeas.europa.eu/policies/eu-cyber-security/> (Zugriff am 5.2.2016).
136 Nato, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, Brüssel 2010, <www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf> (Zugriff am 2.12.2015).
137 »The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence.« Nato, *Wales Summit Declaration*, Pressemitteilung 120/2014, 5.9.2014, <www.nato.int/cps/en/natohq/official_texts_112964.htm> (Zugriff am 3.12.2015).)

Nato Computer Incident Response Capability (NCIRC), die auch mit der operativen IT-Sicherheit und Netzüberwachung betraut ist, alljährlich die dreitägige sogenannte Cyber Coalition.[138] Das NCIRC Coordination Centre ist dabei für die Koordination der Mitgliedstaaten und Partnerorganisationen zuständig, wie der EU, der OSZE oder der Internationalen Fernmeldeunion der VN (International Telecommunication Union, ITU). Auch eine Kooperation der Nato mit dem EU-CERT ist beschlossen.[139] Eine europäische Zusammenarbeit in der Cyberverteidigung schließe neben der Forschung auch die Industrie als »first line of defence« mit ein.[140]

Inklusivität

Streitkräfte können im Cyberraum nur unter denselben verfassungsrechtlichen Voraussetzungen eingesetzt werden, die auch für konventionelle militärische Fähigkeiten gelten. In Deutschland sind dies vor allem Art. 87a GG und Art. 24 Abs. 2 GG. Sind diese Voraussetzungen erfüllt, ist es rechtlich möglich, schädigende (Gegen-)Maßnahmen gegenüber Informationssystemen eines Angreifers zu treffen, einschließlich Informationsgewinnung und Aufklärung. Darüber hinaus kann die Bundeswehr mit eigenen Fähigkeiten zur gesamtstaatlichen Abwehr von IT-Angriffen beitragen. Rechtliche Grundlagen dafür sind die Amtshilfe nach Art. 35 Abs. 1 GG und Bestimmungen über den Einsatz der Bundeswehr zur Abwehr und Bewältigung eines besonders schweren Unglücksfalls. Jeder bewaffnete Einsatz deutscher Streitkräfte erfordert allerdings die Zustimmung des Bundestages nach dem Parlamentsbeteiligungsgesetz.[141] Deshalb empfiehlt es sich, in der Cyberverteidigungspolitik frühzeitig über die Einbindung des Bundestages nachzudenken. Der deutsche Parlamentsvorbehalt ist ein hohes Gut, das nicht leichtfertig dem technologischen Fortschritt geopfert werden darf. In diesem Kontext ist die verspätete Parlamentsbeteiligung zu problematisieren, wie sie in der sogenannten Nafurah-Entscheidung des Bundesverfassungsgerichts[142] im Sommer 2015 legitimiert wurde. Es geht um die Möglichkeit, das Parlament im Falle von Gefahr im Verzug erst im Nachhinein zu unterrichten.

Zivilität

Sorgfaltsverantwortung in der Cyberverteidigung heißt in Friedenszeiten, zum präventiven und reaktiven Schutz der eigenen IT-Systeme und Infrastrukturen vorrangig zivile Ansätze zu verfolgen. Gleichzeitig rüstet sich Deutschland aber militärisch für den Cyberraum. Seit Dezember 2011 verfügt die Einheit für Computernetzwerkoperationen[143] der Bundeswehr über eine Anfangsbefähigung, also einen »Grad der personellen und materiellen Einsatzbereitschaft [...], der es ermöglicht, in begrenztem Umfang, Wirkungen durch den Cyber-Raum zu erzielen.«[144] So unterstehen dem Kommando Strategische Aufklärung (KSA) mehrere Bataillone mit verschiedenen Aufgaben in der elektronischen Kampfführung.[145] Im Zuge der Erstellung des Weißbuchs 2016 verkündete Verteidigungsministerin von der Leyen im September 2015, in der Bundeswehr werde ein Cyber- und Informationsraumkommando (CIRK) aufgebaut.[146] Sicher ist, dass der Cyberraum als fünfter Operationsraum neben Land, Luft, See und Weltraum sich auf die Einsatzfähigkeit der Bundeswehr auswirken wird. Um einen digitalen

138 Zu nennen ist hier auch die Übung »Locked Shields« des CCDCOE.

139 Andreas Wilkens, »EU und Nato kooperieren enger im Kampf gegen Cyber-Terrorismus«, *heise online*, 10.2.2016, <www.heise.de/newsticker/meldung/EU-und-Nato-kooperieren-enger-im-Kampf-gegen-Cyber-Terrorismus-3098911.html?wt_mc=rss.ho.beitrag.atom> (Zugriff am 15.3.2016).

140 So Alexander Vershbow, stellvertretender Generalsekretär der Nato, zitiert auf der Website des Nato Industry Cyber Partnership Forum, <www.nicp.nato.int/> (Zugriff am 3.12.2015).

141 Deutscher Bundestag, *Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland (Parlamentsbeteiligungsgesetz, ParlBG)*, Berlin, 18.3.2005.

142 Anlass war die Beteiligung der Bundeswehr an einer Evakuierungsoperation in Libyen 2011. Bundesverfassungsgericht, *Urteil des Zweiten Senats vom 23. September 2015 – 2 BvE 6/11 – Rn. (1–125)*.

143 Kommando Strategische Aufklärung, *Über uns*, 25.11.2013.

144 Thomas Wiegold, »Cyber-Attacke auch für Deutschland ein möglicher Angriff nach dem Völkerrecht«, *Augen geradeaus!* (Blog), 12.10.2012, <http://augengeradeaus.net/2012/10/cyber-attacke-auch-fur-deutschland-ein-moglicher-angriff-nach-dem-volkerrecht/> (Zugriff am 15.3.2016).

145 Bundesministerium der Verteidigung, *Dienststellen der Streitkräftebasis, Kommando Strategische Aufklärung*, <www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3s4kT9gmxHRQCRV4XQ/> (Zugriff am 30.11.2015).

146 Bundesministerium der Verteidigung, *Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig* [wie Fn. 45]; Bundesministerium der Verteidigung, *Von der Leyen reformiert Cyber-Strukturen* [wie Fn. 133].

Rüstungswettlauf[147] zu verhindern, sollte Cyberverteidigung sich vor allem auf den Aufbau resilienter Strukturen konzentrieren[148], doch mit einer verbesserten Verteidigungsfähigkeit ist es nicht getan. Notwendig ist auch eine Hochsicherheits-IT, die es in enger Zusammenarbeit mit weiteren EU-Staaten und Verbündeten zu entwickeln gilt. Eine weitere wichtige Aufgabe besteht darin, den weltweiten »Schwarzhandel« mit Sicherheitslücken in IT-Systemen einzudämmen und dabei insbesondere Zero-Days-Märkte zu bekämpfen.[149]

Selbst in der Bundeswehr gibt es jedoch Befürchtungen, dass das CIRK eine ähnliche Entwicklung nehmen könnte wie das United States Cyber Command (USCYBERCOM). Dieses ist keinerlei parlamentarischer Kontrolle unterworfen und arbeitet eng mit der NSA zusammen. Es besteht die Sorge, dass die Tätigkeit des CIRK nicht mit dem traditionellen Verständnis vom »Bürger in Uniform« in Einklang zu bringen ist. Entscheidend wird sein, wie die neu zu schaffenden Fähigkeiten strategisch und operational in die Bundeswehr eingegliedert werden sollen.

Internationale Normenentwicklung

Die internationale Normenentwicklung ist ein zentraler Bestandteil deutscher Cyber-Außenpolitik. Deutschland exportiert technologische Produkte in alle Welt und bezieht Vorprodukte aus fast allen Ländern. Vertrauen ins Internet ist daher für die deutsche Wirtschaft unabdingbar. Da die Anpassung an Standards jedoch immer mit Kosten verbunden ist, hat Deutschland ein ausgeprägtes Interesse daran, seine eigenen Standards so weit wie möglich zum internationalen Maßstab zu machen. Zu diesem Zweck setzt die Cyber-Außenpolitik in drei Bereichen an. Erstens strebt sie Vereinbarungen mit Dritten über vertrauens- und sicherheitsbildende Maßnahmen an. Zweitens möchte sie Übereinkommen erzielen, in denen internationale Standards bei der Zulassung von Hard- und Software festgelegt und Normen verantwortlichen staatlichen Verhaltens definiert werden. Drittens macht sie sich für die Anwendung des Völkerrechts im Cyberraum stark.

Europäische Zusammenarbeit

Damit Cyber-Außenpolitik der Sorgfaltsverantwortung im Cyberraum mehr Geltung verschafft, sollte die EU in die Lage versetzt werden, sich stärker in der internationalen Normenentwicklung zu engagieren. Im April 2015 wiesen Federica Mogherini, Hohe Vertreterin der EU für Außen- und Sicherheitspolitik, und der niederländische Außenminister Bert Koenders ausdrücklich darauf hin, dass es notwendig sei, Staaten für ihr Verhalten im Cyberraum in die Pflicht zu nehmen. Die unzureichende Sicherung zentraler Infrastrukturelemente, so Mogherini und Koenders, sei nicht nur eine Bedrohung für die nationale, sondern auch für die internationale Sicherheit.[150] Damit sprechen sie für sämtliche 28 EU-Mitgliedstaaten, die sich auf diese Linie in der Cyberdiplomatie geeinigt haben.[151]

Weil aber die Auffassungen in der Welt über verschiedenste Aspekte der Informationssicherheit weit auseinandergehen, ist eine konstruktive Auseinandersetzung auf globaler Ebene außerordentlich schwierig. Strittig sind etwa der Umfang des Themenfeldes, die Bedrohungswahrnehmung sowie die Rolle der Vereinten Nationen und der Regierungen, auch gegenüber privatwirtschaftlichen und zivilgesellschaftlichen Akteuren. Deutschland ist in all diesen internationalen Debatten prominent vertreten. In der vierten Runde der Regierungsexperten zur Informationssicherheit (VN GGE) verhandelten zwanzig Staaten, davon fünf EU-Mitglieder.[152] Die Abschlussberichte der Experten-

147 Ronald Deibert, »Tracking the Emerging Arms Race in Cyberspace«, in: *Bulletin of the Atomic Scientists*, 67 (2011) 1, S. 1–8.

148 Deutscher Bundestag, 1. Untersuchungsausschuss, *Stenografisches Protokoll der 9. Sitzung*, 18. Wahlperiode, Berlin, 26.6.2014, <www.bundestag.de/blob/372418/97c666605f875474927dfcf5b42c4fcb/09-waidner_gaycken_rieger_endgueltig-data.pdf> (Zugriff am 30.11.2015).

149 »Ein Zero Day Exploit Attack (ZETA) ist ein Angriff, der am selben Tag erfolgt, an dem eine Schwachstelle in einer Software entdeckt wird. In diesem Fall wird die Schwachstelle ausgenutzt, bevor sie vom Softwarehersteller durch einen Fix geschlossen werden kann.« Kaspersky Lab, *Was ist ein Zero-Day-Exploit?*, <www.kaspersky.com/de/internet-security-center/definitions/zero-day-exploit>. Siehe auch Bundesamt für Sicherheit in der Informationstechnik (Hg.), *Die Lage der IT-Sicherheit in Deutschland 2015* [wie Fn. 27].

150 Bert Koenders/Federica Mogherini, »Cyber Space Needs Stronger Rule of Law«, in: *EU Observer*, 16.4.2015, <https://euobserver.com/opinion/128342> (Zugriff am 16.3.2016).

151 Council of the European Union, *Council Conclusions on Cyber Diplomacy*, 6122/15, Brüssel, 11.2.2015.

152 Antigua und Barbuda, Weißrussland, Brasilien (Vorsitz), China, Kolumbien, Ägypten, Estland, Frankreich, Deutschland, Ghana, Israel, Japan, Kenia, Malaysia, Mexiko, Pakistan,

runden wurden durch die Generalversammlung angenommen. Als Konfliktpunkt bleibt die konkrete Anwendung des Völkerrechts auf den Cyberraum bestehen. Ausgewählte EU-Staaten sind auf der VN-Ebene engagiert und vertreten die EU. Eine engere Absprache gibt es unter den »Großen Drei« Europas sowie bilateral mit den USA und Israel in der Gruppe westlicher Gleichgesinnter, zu der neben Deutschland, Spanien, Frankreich und Großbritannien auch Kolumbien, Israel, Japan, Südkorea und die USA zählen. Eine fünfte Runde der GGE-Verhandlungen soll 2016 anlaufen. Die daran beteiligten EU-Staaten sollten ihre Energie darauf konzentrieren, europäischen Belangen in der GGE künftig mehr Nachdruck zu verleihen, wie in den Ratsschlussfolgerungen zur Cyberdiplomatie festgelegt.[153] Dabei muss die Union »mit einer Stimme« sprechen, denn eine gespaltene EU wird große Schwierigkeiten haben, ihre Interessen gegenüber denen der USA, Russlands oder Chinas durchzusetzen.

Inklusivität

Zu den Aufgaben deutscher und europäischer Cyber-Außen- und Sicherheitspolitik gehört es, einen digitalen Rüstungswettlauf zu verhindern, indem zivilen Ansätzen und vertrauensbildenden Maßnahmen Vorrang eingeräumt wird. Anlässlich seiner OSZE-Präsidentschaft 2016 will Deutschland ein neues Paket an vertrauens- und sicherheitsbildenden Maßnahmen für den Cyberraum verabschieden und Wissenschaft und Zivilgesellschaft dabei besonders einbinden.[154] Viele Staaten sehen die OSZE aufgrund ihrer Erfahrungen in blockübergreifender Rüstungskontrolle und Vertrauensbildung als geeigneten Rahmen an, um VSBM in allen drei Körben für den Cyberraum zu entwickeln. Ergänzend zur Arbeit der GGE wird die OSZE als regionaler Ansatz verstanden. Sie soll die gemeinsame Verpflichtung sicherstellen, dass vom Gebiet ihrer Mitgliedstaaten aus keine Computersysteme und Cyberinfrastruktur zu Attacken auf andere Staaten verwendet werden. Ebenso wenig sollen Vorgaben dazu missbraucht werden, die Freiheit des Internets einzuschränken. Gemeinsam mit Wissenschaft und Unternehmen soll die Entwicklung technischer und regulativer Schutzvorkehrungen gefördert werden, um kritische Infrastruktur in OSZE-Staaten widerstandsfähiger zu machen. Cybersicherheit wird nur dann zu gewährleisten sein, wenn die Stakeholder dabei national und europäisch koordiniert vorgehen und möglichst viele Betroffene einbeziehen.[155] Der Multistakeholder-Ansatz kristallisiert sich immer mehr als Markenzeichen der Cyber-Außenpolitik und digitalen Diplomatie heraus.

Zivilität

Die internationale Normenentwicklung wirft politische Fragen auf, die direkte Relevanz für die globale Durchsetzung von Menschenrechten und die nationale Sicherheit haben. Seit Juni 2013 ist Deutschland Mitglied der mittlerweile 28 Länder umfassenden Freedom Online Coalition, die sich als Multistakeholder-Plattform für Freiheiten im Internet einsetzt.[156] Auch deutsche Unternehmen der Informations-, Kommunikations- und Internetwirtschaft unterliegen der Sorgfaltsverantwortung. Deshalb müssen sie dafür sorgen, dass ihre Exportgüter nicht von autoritären Regimen genutzt werden, um Freiheitsrechte im Internet zu missbrauchen. Die Bundesregierung sollte weiter darauf hinarbeiten, dass der Handel mit digitalen Rüstungsgütern weltweit kontrolliert wird.[157] Hierzu

Russland, Spanien, Vereinigtes Königreich, USA.

153 Council of the European Union, *Council Conclusions on Cyber Diplomacy* [wie Fn. 151]; Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012*, Genf: ICT for Peace, 2012.

154 Annegret Bendiek/Christoph Berlich/Tobias Metzger, *Drei Prioritäten für die Cyberdiplomatie unter dem deutschen OSZE-Vorsitz 2016*, Berlin: Stiftung Wissenschaft und Politik, 5.11.2015, (SWP-«Kurz gesagt«), <www.swp-berlin.org/publikationen/kurz-gesagt/drei-prioritaeten-fuer-die-cyberdiplomatie-unter-dem-deutschen-osze-vorsitz-2016.html> (Zugriff am 5.2.2016); Vertretungen der Bundesrepublik Deutschland in der Russischen Föderation, *OSZE-Konferenz zur Cybersicherheit im Auswärtigen Amt*, 18.1.2016, <www.germania.diplo.de/Vertretung/russland/de/__pr/mosk/osze-cyber-konferenz-aa-18012016.html> (Zugriff am 5.2.2016).

155 Siehe Microsoft, *International Cybersecurity Norms*, 2015, <http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf> (Zugriff am 9.12.2015).

156 Freedom Online Coalition, *Freedom Online Coalition Chair's Summary*, Third Freedom Online Conference, Tunis, 16.–18.6. 2013, <www.freedomonlinecoalition.com/wp-content/uploads/2014/04/3-Tunis-Chair-report-from-website.pdf> (Zugriff am 9.12.2015).

157 Deutschland hat den am 2.4.2013 in der Generalversammlung der Vereinten Nationen angenommenen Vertrag über den Waffenhandel ratifiziert. Deutscher Bundestag, *Gesetz zu dem Vertrag vom 2. April 2013 über den Waffenhandel*,

sollten die hochentwickelten Staaten möglichst zügig das Wassenaar-Abkommen[158] zur Waffenexportkontrolle weiterentwickeln, damit der Handel mit digitalen Rüstungsgütern künftig den gleichen Anforderungen unterworfen wird wie schon derjenige mit konventionellem Kriegsgerät. Erste Schritte wurden bereits getan, um internationale Mechanismen der Exportkontrolle einzuführen und Überwachungstechnologien in Sanktionsregime aufzunehmen. Diese Ansätze könnten zumindest auf regionaler Ebene mit Hilfe der Dual-Use-Verordnung der EU[159] weiter vorangetrieben werden. Vor allem die Ausfuhr solcher Produkte in autoritär regierte Länder sollte rigider unterbunden werden als bisher. Zu diesem Zweck müssen eine einheitliche Definition von Cyberwaffen erarbeitet und Überwachungsregime auf den Ebenen der EU und der VN konzipiert werden.[160] Derzeit ist nicht zu erwarten, dass Regierungen auf multilateraler Ebene völkerrechtliche Verträge schließen, in denen die Nutzung des Cyberraums für militärische Operationen nach dem Muster von Abrüstung und Rüstungskontrolle verbindlich geregelt wird. Als Gründe dafür gelten die fehlende Definition des Begriffs Cyberwaffen, Implementierungs- und Verifikationsprobleme sowie die Schwierigkeit, Cyberangriffe völkerrechtlich eindeutig zuzuordnen. Bilaterale Abkommen wie die Vereinbarungen zwischen den USA und China zur Cyberkriminalitätsbekämpfung lassen sich offenbar leichter durchsetzen.[161] Grundsätzlich sollte die Sorgfaltsverantwortung als wechselseitig verstanden werden. Das hieße, dass Normen und Regeln zwischen einzelnen Staaten sowie zwischen Staaten und privaten Unternehmen gelten sollen, vor allem im Hinblick auf Spionage und weitere militärische Zwecke wie etwa hybride Kriegsführung. Ein heikles Thema in der Kooperation zwischen zivilen und militärischen sowie öffentlichen und privaten Akteuren ist die Dual-Use-Technik, besonders in der transatlantischen Abstimmung. Die euro-atlantische Zusammenarbeit wäre ein guter Auftakt, um Staaten innerhalb der EU und des Bündnisses darauf festzulegen, Schwachstellen in IT-Produkten den Herstellern zu melden, statt selbst bei Bedarf absichtlich Hintertüren einzubauen. Es lässt sich nicht bestreiten, dass es gängige Praxis ist, Cyberwaffen wie etwa Zero-Day-Attacken einzusetzen. Zumindest ihre Anwendung aber sollte stärker limitiert werden, also klare Kriterien erfüllen müssen. Auf jeden Fall unterbunden werden sollte die Verbreitung von Cyberwaffen.

Berlin, 19.10.2013.

158 Siehe *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, Den Haag, 19.12.1995, <www.wassenaar.org/december-1995-declaration-at-the-peace-palace-the-hague/> (Zugriff am 5.2.2016).

159 Council of the European Union, *Council Regulation (EC) No. 428/2009 on Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items*, Brüssel, 5.5.2009.

160 Zurzeit gibt es keine international gültigen Definitionen für den Cyberraum. Das Cyber-Abwehrzentrum der Nato hat auf Basis des Tallinn Manual eine Liste der in der Allianz gebräuchlichen Definitionen zusammengetragen. CCDCOE, *Cyber Definitions*, <https://ccdcoe.org/cyber-definitions.html> (Zugriff am 5.2.2016).

161 Julie Hirschfeld Davis/David E. Sanger, »Obama and Xi Jinping of China Agree to Steps on Cybertheft«, in: *The New York Times*, 25.9.2015, <www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html?_r=0> (Zugriff am 5.2.2016).

Sorgfaltsverantwortung (noch besser) implementieren

Die deutsche Cyber-Außenpolitik bedarf einer strategischen Neuorientierung, die den deutschen Interessen Rechnung trägt. Als europäische Mittelmacht kann Deutschland diese neue Ausrichtung nur in einer Perspektive finden, die mit seiner Eingebundenheit in Europa, seinen demokratischen Werten und seinem festen Bekenntnis zu zivilen Politikformen im Einklang steht. Dafür bietet sich die Norm der Sorgfaltsverantwortung an. Sie ist Ausdruck des kooperativen und globalen Charakters einer guten Cyber-Außen- und Sicherheitspolitik, ohne deren innenpolitisches Fundament zu verbergen. Moderne (Cyber-)Außen- und Sicherheitspolitik ist immer zugleich auch Innenpolitik.

In der deutschen Cyberpolitik wurde damit begonnen, das Prinzip der Sorgfaltsverantwortung umzusetzen. Seine Grundidee ist, dass Staaten Verantwortung für die von ihrem Territorium ausgehenden Bedrohungen übernehmen und zusammen mit anderen EU-Staaten und Verbündeten alles in ihrer Macht Stehende tun, um eine Schädigung Dritter zu verhindern. Die Entwicklung der deutschen Cybersicherheitsstrukturen bewegt sich schon einen großen Schritt in diese Richtung. Sie sind zumindest ansatzweise europäisch ausgerichtet und bringen eine Vielzahl interessierter Parteien zusammen. Auch in der digitalen Industriepolitik finden sich Kooperationen zwischen staatlichen und privaten Akteuren mit dem Ziel, Fachkompetenz zu bündeln und der Sorgfaltsverantwortung Gewicht zu verleihen. Der Vorrang des Zivilen vor dem Militärischen ist in beiden Bereichen ausgeprägt.

Gleichwohl bleibt eine Reihe von Ansatzpunkten, die deutsche Cyber-Außen- und Sicherheitspolitik zu verbessern:

Erstens: Die Norm der Sorgfaltsverantwortung muss in den internationalen Beziehungen nachhaltig durchgesetzt werden. Bisher hat sie lediglich den Status einer umstrittenen Rechtsnorm und findet sich nicht als verbindliche Bestimmung in bilateralen und multilateralen Übereinkünften wieder. Im Abschlussbericht der vierten Runde der Regierungsexperten zur Informationssicherheit (VN GGE) bekennen sich die dort vertretenen Staaten dazu, Angriffe vom eigenen Territorium zu unterbinden und nicht absichtlich die kritische Infrastruktur oder IT-Notfallteams anderer Länder zu beeinträchtigen. Auch das Abkommen zwischen China und den USA zur gemeinsamen Bekämpfung der Cyberkriminalität und zum Verbot von Industriespionage ist ein vielversprechender Schritt, der als Vorbild für bilaterale Abkommen anderer Länder dienen kann. Hier gilt es sowohl politisch auf eine allgemeine Anerkennung der Sorgfaltsverantwortung hinzuarbeiten als auch mittelfristig die nötigen institutionellen Strukturen zu schaffen, um eine effektive Anwendung der Norm zu gewährleisten. Eine Hauptrolle bei der europäischen Koordinierung einer Cyber-Außen- und Sicherheitspolitik spielt das Auswärtige Amt. Als einziges Ressort steht es über den partikularen Sichtweisen einzelner Politikfelder und kann als Querschnittministerium die unterschiedlichen justiz-, innen- und wirtschaftspolitischen Fragen auch auf EU-Ebene zusammendenken.

Die deutsche Cyber-Außen- und Sicherheitspolitik sollte noch stärker innerhalb der EU-Strukturen formuliert werden. Nur im und durch den EU-Binnenmarkt kann Deutschland international mit dem notwendigen Nachdruck agieren. Ein erfolgversprechender Ansatzpunkt ist die Friends of the Presidency Group (FoP) on Cyber Issues. Sie wurde 2013 ins Leben gerufen, um die Umsetzung der EU-Cybersicherheitsstrategie zu unterstützen. Hier werden die verschiedenen Cyberthemen horizontal auf EU-Ebene koordiniert. Die Arbeitsgruppe ist bisher zwar nur für jeweils drei Jahre eingerichtet worden, hat sich aber schon als wichtigste Drehscheibe für die Abstimmung nationaler Interessen in der europäischen Cyberpolitik etabliert.

Zweitens: Auf allen Themenfeldern ist deutlich geworden, dass EU und USA in Regelungsfragen den Ton angeben. Wenn sie sich einig sind, können sie genug politischen Einfluss in die Waagschale werfen, um die Sorgfaltsverantwortung wirkungsvoller durchzusetzen. Dringend nötig ist eine transatlantische Initiative, die sich mit der Attributionsproblematik befasst, also der Schwierigkeit, Cyberangriffe zweifelsfrei einem Akteur zuzuordnen. Staaten nutzen diese nämlich vielfach als Ausweg aus der Sorgfaltsverantwortung, indem sie die Schuld auf Dritte abwälzen. Parallel zu den TTIP-Verhandlungen wäre nicht nur der wirtschaftliche Datentransfer, sondern auch ein

innen- und justizpolitisches transatlantisches Abkommen auf den Weg zu bringen, mit dessen Hilfe strafrechtliche Normen harmonisiert, der Datenaustausch geregelt und alle weiteren einzelstaatlichen Maßnahmen eingeleitet werden können. Die Datenschutzgrundverordnung der EU sollte zügig um den Privatsphäre-Schutzschirm (Privacy Shield) ergänzt werden, auf den EU und USA sich verständigt haben. Bei der Umsetzung des Privacy Shield sollten die rechtlichen Vorbehalte der EuGH-Entscheidung vom Oktober 2015 berücksichtigt werden. Nur so lässt sich Unternehmen und Verbrauchern die nötige Rechtssicherheit geben. Mit der Einigung auf eine Datenschutzgrundverordnung hat die EU zwar das Problem entschärft, dass Daten europäischer Bürger nach US-Recht gespeichert und ausgewertet werden können. Allerdings hat sie damit auch einen fragwürdigen Präzedenzfall extraterritorialer Wirkung eigenen Rechts gesetzt, und das, obwohl sie eine solche Praxis zuvor bei den USA kritisiert hat. Globale Unternehmen müssen ihre Daten europäischer Bürger heute faktisch in Europa speichern, um nicht in Konflikt mit EU-Recht zu geraten. Die EU hat mit ihrer Entscheidung signalisiert, dass sie in der Anwendung eigenen Rechts auf fremdem Hoheitsgebiet kein Problem sieht. Unausgesprochen hebelt sie damit die Sorgfaltsverantwortung gegenüber Dritten aus. Staaten wie die USA oder China dürften deshalb künftig wenig Skrupel haben, ebenfalls Rechtsbestimmungen mit extraterritorialer Wirkung zu erlassen. Dies könnte eine Kollision unterschiedlicher nationaler Rechtssysteme zur Folge haben, welche die Fragmentierung des globalen Wirtschaftsraums und des Internets fördern würde. Das Privacy Shield zum Datentransfer und das transatlantische Abkommen zum Datenschutz in der Strafverfolgung sind daher notwendige Schritte im Bestreben, diesen Prozess zu stoppen.

Drittens: Sorgfaltspflichten sollten denjenigen Staaten auferlegt werden, die angegriffen wurden, auf deren Gebiet die angegriffenen Server stehen oder über deren Datenleitungen Angriffe verübt werden. Die Pflichtendichte sollte sich nach den Einflussmöglichkeiten und Internetkapazitäten der betroffenen Staaten richten. Sinnvoll erscheint auch, das materielle Strafrecht zu modifizieren und zur Abschreckung zu nutzen. Darüber hinaus sollte insbesondere die IT-Forensik ausgebaut werden, um die Urheber von Cyberattacken besser identifizieren zu können. Hier sind nichtstaatliche Akteure zur aktiven Mitwirkung aufgefordert. Wenn Unternehmen aufgrund unterschiedlicher nationaler Rechtsanforderungen zum Rechtsbruch gezwungen werden (zum Beispiel durch ein zu befolgendes staatliches Auskunftsverlangen auf der einen, ein Herausgabeverbot aus Datenschutzgründen auf der anderen Seite), werden die beteiligten Staaten dem Prinzip der Rechtsstaatlichkeit nicht gerecht. Aus der Erfahrung der europäischen Integration heraus wäre es empfehlenswert, nach dem Modell des Europäischen Gerichtshofs eine supranationale Gerichtsbarkeit oder Schiedsgerichte mit Kompetenzen auszustatten, um der Sorgfaltsverantwortung in diesem Punkt mehr Geltung zu verschaffen. Auf diese Weise ließe sich auch die Rechtsunsicherheit für Unternehmen verringern. Auf der anderen Seite müssen Unternehmen darauf verpflichtet werden können, ihre Softwareprodukte sicherer zu machen. Zumindest müssen die Kriterien für Transparenz, Test und Analyse verschärft werden.

Viertens: Die wachsende Komplexität IT-geschützter Waffensysteme und die mittlerweile erreichte Qualität festgestellter Cyberangriffe erfordern viel Know-how in der Cybersicherheit. Darüber hinaus muss die wehrtechnische Industrie Datensicherheit schon beim Design der jeweiligen Systemarchitektur mitberücksichtigen. Deswegen liegt es nahe, die Hersteller bei der Weiterentwicklung und -nutzung von Cyber-Verteidigungssystemen einzubeziehen. Das sollte indes nur in europäischer Abstimmung geschehen, durch politisch unabhängige beziehungsweise parlamentarische Entscheidungen legitimiert werden und allein der militärisch defensiven Logik verpflichtet bleiben. Andernfalls widerspräche ein solches Handeln der Sorgfaltsverantwortung und würde auch mit der außen- und sicherheitspolitischen Tradition militärischer Zurückhaltung brechen. Zur geforderten Inklusivität in allen Fragen der Cyber-Außen- und Sicherheitspolitik gehört es, den Bundestag gebührend zu beteiligen. Soll die Bundeswehr befähigt werden, Cyberabwehr auch mit digitalen Angriffen zu betreiben, wäre der dafür womöglich notwendige politische Kurswechsel im Parlament zu diskutieren. Sicherheitspolitische Widerstandsfähigkeit setzt gesellschaftliche Resilienz voraus, die nur durch öffentliche Diskussionen erzeugt werden kann. Hierzu gehört auch, den Parlamentsvorbehalt für den Fall von Cyberoperationen der Bundeswehr einer Realitätsprüfung zu unterziehen. Aufgabe des Bundestages ist es, effektive parlamentarische Strukturen zur Kontrolle zu schaffen.

Abkürzungsverzeichnis

AA	Auswärtiges Amt
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPS	Child Abuse Prevention System
CCDCOE	Cooperative Cyber Defence Centre of Excellence (Nato)
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung
CERTBw	Computer Emergency Response Team der Bundeswehr
CIRK	Cyberinformationsraumkommando
CNA	Computer Network Attacks
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computernetzwerkoperation
COMPACT	*C*ivic Responsibilities, *O*ne Unfragmented Resource, *M*ultistakeholder Approach to *P*romote Democracy and Human Rights, Sound Technological *A*rchitecture, *C*onfidence and *T*ransparent Governance
CSIRT	Computer Security Incident Response Team
DSGVO	Datenschutzgrundverordnung (EU)
EAD	Europäischer Auswärtiger Dienst
EFTA	European Free Trade Association
EGC	European Government CERTs Group
ENISA	European Network and Information Security Agency
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurojust	European Union's Judicial Cooperation Unit
Europol	Europäisches Polizeiamt
FIRST	Forum for Incident Response and Security Teams
FoP	Friends of the Presidency Group on Cyber Issues
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (VN)
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IGF	Internet Governance Forum
IKT	Informations- und Kommunikationstechnologie
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informationstechnik
IWWN	International Watch and Warning Network
KMU	Kleine und mittlere Unternehmen
KSA	Kommando Strategische Aufklärung
MAD	Militärischer Abschirmdienst
NIS	Network and Information Security
NIST	National Institute of Standards (USA)
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PKGr	Parlamentarisches Kontrollgremium
PNR	Passenger Name Record
PPP	Public-Private Partnership
SIGINT	Signals Intelligence
SIT	Strategische Initiative Technik
SWP	Stiftung Wissenschaft und Politik
TA	Technische Aufklärung
TFTP	Terrorist Finance Tracking Programme
TKÜ	Telekommunikationsüberwachung
TTIP	Transatlantic Trade and Investment Partnership
UP KRITIS	Umsetzungsplan für (kritische) Infrastrukturen
VN	Vereinte Nationen
VSBM	Vertrauens- und sicherheitsbildende Maßnahmen
WEF	World Economic Forum
WSIS	World Summit on the Information Society
ZKA	Zollkriminalamt

Lektüreempfehlungen

Annegret Bendiek/Christoph Berlich/Tobias Metzger
Die digitale Selbstbehauptung der EU
SWP-Aktuell 71/2015, August 2015

Christian Schaller
Internationale Sicherheit und Völkerrecht im Cyberspace
SWP-Studie 18/2014, Oktober 2014

SWP Berlin
Sorgfaltsverantwortung im Cyberraum
März 2016