„Zur Sorgfaltsverantwortung im Cyberraum. Anforderungen an eine neue deutsche Cyber-Sicherheitsstrategie“*

Annegret Bendiek

English titel: Due Diligence in Cyberspace. Needs for a New German Strategy for Cybersecurity

Abstract: Global cyber-space is undergoing fundamental change. There are now frequent references to a “fragmentation of the Internet”, but many European and international working groups are also increasingly aware that “a free, open and at the same time secure Internet” is a global public asset. However, the political rules adopted for international cyber policies and cyber-security policies will always lag behind technological developments. It is the more important, therefore, to subject these rules to the overarching norm of due diligence in cyber-space, and to do so on the national, European and international levels. This leads to three requirements for Germany’s future strategic orientation in cyber-space: European cooperation: integrating national policies into the European framework; inclusiveness: giving different interest groups broad and publicly accessible representation in formulating policies; and civil society: prioritising the civilian component over the military component, particularly in times of peace.

Keywords: Due diligence, cyberspace, Cyber Foreign and Security Policy
Stichwörter: Sorgfaltsverantwortung, Cyber- und Informationsraum, Cyber-Außen- und Sicherheitspolitik

1. Einleitung[1]

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 Regelsetzungsversuchen verlangt. Allerdings plädieren auch immer mehr politische Stimmen für eine Renationalisierung politischer Regulierung und digitale Souveränität. Die Politik muss sich der Realität stellen, dass der Cyberraum vermehrt zum Operationsfeld des Militärs wird.

Das neue Weißbuch der Bundesregierung, die Globale Strategie für die Außen- und Sicherheitspolitik der EU sowie die NATO-EU-Kooperation zur Cyberverteidigung bringen die Tendenz zur Versicherheitlichung des Informationsraums zum Ausdruck. An welchen übergeordneten Normen sollte sich die deutsche und europäische Außen- und Sicherheitspolitik im Cyberraum ausrichten?

2. Die Sorgfaltsverantwortung als Leitidee

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 ein globales öffentliches Gut beschreiben, zu dessen Bereitstellung die Kooperation aller wichtigen Staaten, Unternehmen, Wissenschaftsvertreter und der Zivilgesellschaft nötig ist. Regionale Fragmentierung, Gefährdungen durch Kriminalität und eine Militarisierung des Cyberraums werden nur dann zu verhindern sein, wenn die Staatengemeinschaft einschließlich aller Stakeholder im Internet 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 Cyberraums auf ein tragbares Maß reduziert sind“[3].

Die Bundesregierung, die Mitgliedstaaten sowie die EU folgen prinzipiell der Idee von „Due-Dilligence“[4] bei der Umsetzung ihrer Cybersicherheitsstrategien. Diese Norm hat sich bereits im Umweltrecht bewährt und verpflichtet Staaten, (für Sicherheitsbereich in *Friedenszeiten)* dafür zu sorgen, dass von ihrem Territorium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen.[5] Die Bundesregierung stellt in ihrer Cybersicherheitsstrategie den präventiven und reaktiven Schutz der IT-Systeme und Infrastrukturen sowie zivile, polizeiliche und militärisch-defensive Ansätze in den Vordergrund. Im Jahr 2000 hat die Generalversammlung der Vereinten Nationen Staaten dazu aufgefordert, „[to] ensure their laws and practice eliminate safe havens for those who criminally misuse information

* Dieser Beitrag wurde anonym begutachtet (double-blind peer reviewed).

1 Dieser Manuskriptvorschlag ist die überarbeitete und gekürzte Version der SWP-Studie „Sorgfaltsverantwortung im Cyberraum. Leitlinie für eine deutsche Cyber-Außen- und Sicherheitspolitik“, S. 3, März 2016.

2 *Die Bundesregierung*, Europäische und internationale Dimension der Digitalen Agenda, http://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/7_Dimension/dimension_node.html (abgerufen am 16.9.2016).

3 Cyber-Sicherheitsstrategie für Deutschland, S. 15. Vgl. auch Hans-Jürgen Lange, Astrid Böttcher, Cyber-Sicherheit, Springer VS, 2015.

4 Dies geht zurück auf das Urteil des International Court of Justice, The Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania, The Corfu Channel Case (Merits), Judgment of April 9th, 1949, S. 4-38);

5 *Michael N. Schmitt* (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013; vgl. Bundesministerium des Innern (Hrsg.), Cybersicherheitsstrategie für Deutschland, 2011, S. 12.

technologies".[6] Der Internationale Gerichtshof führt in einem Urteil weiter aus, »dass die Verpflichtung zur Prävention eine Pflicht zur Sorgfalt« ist.[7] 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".[8] 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.[9]

„Due Diligence" wird in völkerrechtlichen Abhandlungen zumeist mit dem Begriff Sorgfaltspflicht übersetzt.[10] Dieser verweist allerdings lediglich auf Restriktionen, denen das eigene Handeln unterliegt. Sinnvoller ist es, Due Diligence als »Sorgfaltsverantwortung« zu fassen. Der Grundsatz der Due-Dilligence entfaltet nämlich seine 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. 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.[11]

Cyber-Außen- und Sicherheitspolitik im Sinne der Sorgfaltsverantwortung schließt also die Art und Weise politischer Regulierung ein. Die deutsche Cyber-Außen- und Sicherheitspolitik ist als recht neuer Kernbereich der EU und Nato-Zusammenarbeit zu verstehen und ist demzufolge europäisch zu koordinieren, zu militärischer Zurückhaltung verpflichtet sowie in inklusive und transparente Regelsetzungsprozesse einzubinden.

Zur Sorgfaltsverantwortung[12] gehört erstens, dass Regelsetzungsprozesse ein hohes Maß an Repräsentativität und Inklusivität sowie Transparenz aufweisen müssen, um der Verantwortung für die eigenen Regelungen und deren Auswirkungen auf Dritte Rechnung tragen zu können.[13] Die Inklusivität von Rechtsetzungsprozessen sollte auch dort enden, wo privatwirtschaftliche Akteure beginnen, maßgeblichen Einfluss auf gesetzgebende Organe auszuüben.[14] Gegensteuern lässt sich nur mit transparenten und repräsentativen Verfahren, die auch anderen Staaten ein Mindestmaß an Gewissheit geben, dass ihre legitimen Interessen berücksichtigt werden. 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, sodass 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 unterbinden.

Eine zweite Maxime des deutschen außenpolitischen Selbstverständnisses lautet, Regelsetzungen möglichst präzise mit den wichtigsten europäischen Partnern abzustimmen. Im Rahmen der europäischen Integration ist das Prinzip der Sorgfaltsverantwortung auch mit den europäischen Pflichten zur Politikkoordination in Einklang zu bringen. Wie die Außen- und Sicherheitspolitik ist auch der europäische Wirtschaftsraum durch digitale Technologien derart stark vernetzt, dass einzelstaatliche Maßnahmen allein wenig Sinn ergeben. Deutsche Maßnahmen zur Förderung des Zieles eines freien und sicheren Internets sollten daher immer zumindest europäisch bzw. 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 intensiv die EU-Strukturen nutzt, etwa die Gruppe der Freunde der Präsidentschaft (Friends of the Presidency Group on Cyber Issues, FoP Cyber).[15] 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 drittens aus historischen Gründen selbstverständlich, jeglicher Militarisierung des Cyberraums[16]

6 United Nations Resolution 55/63, Combating the criminal misuse of information technologies, Januar 2001, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (abgerufen am 16.9.2016).

7 *International Court of Justice*, Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20.4.2010, ICJ Reports 2010, S. 14-107 (79) [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«.

8 Artikel 28 ff. 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, 2001, Vol. II, Part Two, S. 26–143; veröffentlicht auch als Annex zu UN General Assembly, Resolution 56/83, Responsibility of States for Internationally Wrongful Acts, 12.12.2001, UN-Dok. A/RES/56/83 vom 28.1.2002.

9 *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, Juni 2015, UN-Dok. A/70/174.

10 Zum Völkerrecht des Netzes siehe *Christian Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, Oktober 2014.

11 Siehe hierzu auch die Studie des Berkman Center for Internet and Society at Harvard „Don't Panic: Making Progress on the ‚Going Dark' Debate", 2016 sowie die Berichte der ENISA.

12 Christopher Daase, Julian Junk (Hrsg.), Internationale Schutzverantwortung – Normative Erwartungen und politische Praxis, Sonderheft der „Friedens-Warte – A Journal of International Peace and Organization", 88 (2013); Hanns W. Maull, *What German Responsibility Means*, in Security and Human Rights, 26 (2015), 11-24.

13 *Christopher Daase*, Vortrag zum CyberLab im September 2015.

14 *Patrick Beuth*, Bundesregierung hofiert Lobbyisten, 10.03.2015, http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag (abgerufen am 16.9.2016)

15 Die Gruppe wurde 2013 ins Leben gerufen, um die EU-Cybersicherheitsstrategie zu unterstützen. Hier werden die verschiedenen Cyberthemen horizontal koordiniert.

16 Siehe hierzu einschlägig *Ron Deibert:* Black Code: Inside the Battle for Cyberspace, Toronto 2013; Miriam Dunn Cavelty: Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London, Routledge 2008. Zuletzt Paper "Cyber-Security and the Negative Consequences of State Action" written for the SWP Conference "The Future of International Order", Berlin, 29.11.-1.12.2015.

entgegenzuwirken – trotz der unumstrittenen Notwendigkeit defensive „Hochwertfähigkeiten" vorhalten zu können, um der Sorgfaltsverantwortung des Staates sowie der Bündnisfähigkeit Rechnung zu tragen. Sorgfaltsverantwortung heißt auch, in den Kategorien globaler öffentlicher Güter zu denken. Deshalb ist es unerlässlich, die deutsche Tradition der Zivilmacht auch in der Cyber-Außen- und Sicherheitspolitik fortzusetzen und ihre Interessen mit ökonomischen und politischen statt mit militärischen Mitteln zu verfolgen. Militärische Gewalt – also auch eine offensive Cyberverteidigung[17], 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)[18] befördern, mit unkalkulierbaren Konsequenzen für verwundbare kritische Infrastrukturen.

3. Die 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. 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.[19] Die Entwicklung ausdifferenzierter Zuständigkeiten zur gesamtstaatlichen Sicherheitsvorsorge ist politisch gewollt. 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. In der deutschen Cyber-Außen- und Sicherheitspolitik finden 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 Fragen der Cybersicherheit in Deutschland liegt im BMI.[20] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale 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.[21] 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).[22] 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.[23]

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. Darin sind das Bundesamt für Sicherheit in der Informationstechnik (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 vertreten.[24] Die Informationsplattform soll die Zusammenarbeit zwischen den Behörden vereinfachen und Schutz- und Abwehrmaßnahmen gegen IT-Angriffe optimieren. Darüber hinaus ist das Abwehrzentrum Bestandteil der projektbasierten Zusammenarbeit mit Unternehmen und Dienstleistern sowie mit Sicherheitsbehörden im Ausland. 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. Mit diesen Informationen unterstützt der BND auch die Bundeswehr.

Dritter Pfeiler: Nationaler Cyber-Sicherheitsrat

Beim Umgang mit den Herausforderungen der Cybersicherheit soll eine starke gesamtstaatliche Koordination gewährleistet bleiben.[25] Zu diesem Zweck versammeln sich im Nationalen

17 Vgl. Kleine Anfrage der Abgeordneten *Dr. Alexander Neu* u.a.: Krieg im „Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung, Deutscher Bundestag, BT-Drucksache 18/6496 vom 16.10.2015. Zur Klassifizierung siehe auch *Robert S. Dewar*: The Triptych of Cyber Security. A Classification of Active Cyber Defence, 2014 6th International Conference on Cyber Conflict.

18 Das Ziel eines solchen Angriffs ist es, möglichst lange unentdeckt zu bleiben, um sensible Informationen auszuspähen oder sogar zu sabotieren.

19 *Bundesministerium des Innern* (BMI) (Hrsg.), Cyber-Sicherheitsstrategie für Deutschland, [wie Fn. 10].

20 *Bundesministerium der Verteidigung*. *Weißbuch 2016*, http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK-9pNyydL3y1Mzi4qTS5Az9gmxHRQBg2ftX/ (abgerufen am 30.11.2015).

21 *Bundesministerium für Justiz und für Verbraucherschutz* (BMJV), Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), Juli 2015, http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (abgerufen am 16.9.2016).

22 *International Watch and Warning Network*, Overview, http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network (abgerufen am 16.9.2016).

23 *Bundesamt für Sicherheit in der Informationstechnik* (BSI), Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (abgerufen am 30.11.2015).

24 *Bundesministerium des Innern* (BMI), Nationales Cyber-Abwehrzentrum, http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html (abgerufen am 30.11.2015).

25 PITS 2013: IT-Sicherheit föderalisiert sich, Oktober 2013.

Cyber-Sicherheitsrat ressortübergreifend die Staatssekretäre unter dem Vorsitz des Beauftragten der Bundesregierung für Informationstechnik.[26] 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 (BMBF), 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). 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.[27] 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.[28] 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.

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«.[29] Hierfür sind die CNO-Kräfte (Computer-Netzwerkoperation)[30] der Bundeswehr zuständig, die weiter ausgebaut und künftig zur aktiven Cyberverteidigung eingesetzt werden sollen. Für präzise militärische Cyberoperationen ist derzeit der Aufbau eines Pools von IT-Reservisten in Planung.[31] 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.[32] 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«.[33]

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. Diese innenpolitischen Anpassungen wären im Sinne der Sorgfaltsverantwortung umzusetzen.

1. 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. Zu fragwürdigen Praktiken der Geheimdienste, etwa zur Industriespionage und dem Führen sogenannter Selektorenlisten mit Ausspähzielen 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.
2. 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.[34] Wichtige Partner Deutschlands wie Frankreich oder die Niederlande bemängeln, oft sei nicht nur unklar, was »die deutsche Position« eigentlich vorsehe, sondern auch, mit welchem Ministerium in der europäischen Abstimmung zu verhandeln sei.

26 *Bundesministerium des Innern* (BMI), *Cyber-Sicherheitsrat*, http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cybersicherheitsrat/cybersicherheitsrat_node.html (abgerufen am 16.9.2016).

27 *Bundesministerium des Inneren*, Cyber-Sicherheitsstrategie für Deutschland, Februar 2011, http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html (abgerufen am 16.9.2016).

28 *Auswärtiges Amt*, Cyber-Außenpolitik, 13.11.2015, http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html (abgerufen am 05.02.2016).

29 *Bundesministerium der Verteidigung* (BMVg) (Hrsg.), Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig, http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYuxDsIwDET_yE5gKWwtZWBhYI-GypW0UGTVOZZyy8PEkA3fSG-7p8Iml7DYKTimxW_CBw0TH8QNj3A-K8UpayQiSmt3qhHPFeP7OHKbHXSvWsVBjEaRJYk-hSTRYpBmjGwdi-M9b8Y7_t7nw9nJpm31-6G64xtj-fkO2W/ (abgerufen am 16.9.2016).

30 Computernetzwerkoperationen (CNO) sind nicht-kinetische Angriffsmittel, die ihre Wirkung durch den Einsatz von Computercode 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.

31 *Bundesministerium der Verteidigung* (BMVg) (Hrsg.), Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig, [wie FN. 12].

32 *Andre Meister*, Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe, 30. Juli 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/ (abgerufen am 30.11.2015).

33 „Geheimhaltung versus Transparenz", in: Behörden Spiegel, 15. November 2015, S. 48.

34 In der Europäischen Union besteht seit 2011 im Geschäftsbereich des Europäischen Auswärtigen Dienstes das sogenannte EU Intelligence Analysis Centre (EU INTCEN). Es ist eine in der EU einmalige Einrichtung, die auf Zulieferung nationaler Nachrichtendienste, zivile Lageanalysen für EU-Entscheidungsträger zur Verfügung stellt. (EEAS, EUINTCEN Fact Sheet, 05.02.2015, http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf, Zugriff am 05.02.2016).

3. Nachgelagerte Behörden wie BSI, BKA und BND haben bereits grundlegende institutionelle Anpassungen zur Abwehr von Cyberangriffen vorgenommen. Die vieldiskutierte institutionelle Abhängigkeit des BSI vom BMI bleibt indes bestehen. 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«.[35] Außerdem greifen nur wenige Unternehmen auf IT-Beratung durch staatliche Stellen zurück. Ferner würden sich Unternehmen, die Opfer von Cyberangriffen geworden seien, eher an die Verfassungsschutzämter als an die Polizei wenden.

4. 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«.“[36] Die Bundesregierung ist der Auffassung, dass noch reichlich ungenutzte Potenziale 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.[37] Bei der Digitalisierung sind jedoch andere Länder erfolgreicher. Vorreiter sind überwiegend US-amerikanische, südkoreanische und chinesische Unternehmen. Die Bundesregierung hat seit 2014 vielfältige Programme wie etwa die Digitale Agenda aufgelegt, mit denen sie global Anschluss zu finden hofft. 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.

4.1 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. Der Schutz kritischer Infrastrukturen zum Beispiel wurde in Deutschland 2007 in Form des UP KRITIS eingeführt, einer öffentlich-privaten Partnerschaft von Betreibern solcher Infrastruktur. Auf EU-Ebene wurde der Richtlinienentwurf zur Netz- und Informationssicherheit im Juli 2016 verabschiedet. Die IT-Sicherheit bei Betreibern kritischer Infrastrukturen und großen Online-Dienstleistern soll verbessert werden. Betroffene Unternehmen müssen Sicherheits- und Datenschutzvorfälle sowie IT-Angriffe melden. Die Auflagen gelten für sämtliche Betreiber und Anbieter »essentieller Dienste«, 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 Digitalunternehmen sollen generell 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 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 bereits das IT-Sicherheitsgesetz im Juli 2015 und führte damit schon früher Meldepflichten bei schwerwiegenden Cyberangriffen und Mindeststandards für den Schutz kritischer Infrastrukturen ein. Betreiber solcher Infrastrukturen müssen seit Juni 2015 einen Mindeststandard an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Zur Steigerung der IT-Sicherheit im Internet sind die Anforderungen an die Anbieter von Telekommunikations- und Telemediendiensten erhöht worden. Die Kompetenzen des BSI und der Bundesnetzagentur und die Ermittlungszuständigkeiten des Bundeskriminalamtes im Bereich der Computerdelikte sind ausgebaut worden.

4.2 Europäisierung

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. Aus der Wissenschaft wurde Kritik laut, »der Diskurs zu Industrie 4.0 [verlaufe] häufig zu technisch und national«.“[38] Daher sei dieser Diskurs stärker als bisher mit der EU-Ebene zu verzahnen, denn bei (kritischen) Infrastrukturen würden Lösungen zu Datensicherheit, Betriebssicherheit und Datenschutz bislang nicht zusammengeführt.[39] Das spiegelt sich auch im Programm Digitale Agenda 2014–2017 der Bundesregierung wider. Zu den dort skizzierten sieben Handlungsfeldern gehört die »europäische und internationale Dimension«.[40] Laut Koalitionsvertrag soll

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

36 *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung. Strategie Intelligente Vernetzung, September 2015, < http://dip21.bundestag.de/dip21/btd/18/060/1806022.pdf> (abgerufen am 30.11.2015).

37 Deutscher Bundestag, IKT-Potentiale nicht ausgeschöpft, Oktober 2015, < https://www.bundestag.de/presse/hib/2015_10/-/390352> (abgerufen am 16.9.2016).

38 *Sabine Pfeiffer*, Industrie 4.0 und die Digitalisierung der Produktion – Hype oder Megatrend? In APUZ, 31-32/2015, S. 6-12.

39 So Peter Liggesmeyer, Leiter des Frauenhofer-Instituts für experimentelles Software Enginering und Präsident der Gesellschaft für Informatik im Ausschuss Digitale Agenda, 1. Juli 2015.

40 *BMWi, BMI, BMVI*, Digitale Agenda 2014-2017, August 2014, http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6 (abgerufen am 16.9.2016).

zwar ein »europäischer Vertrauensraum« geschaffen werden[41], aber vorrangig mit Hilfe nationaler »Maßnahmen zur Rückgewinnung der technologischen Souveränität«: „[Wir] unterstützen die Entwicklung einer vertrauenswürdigen IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie".[42] Die Europäische Kommission hat im Mai 2015 eine Strategie für den digitalen Binnenmarkt vorgelegt. [43] Die Industriepolitik 4.0 auf EU-Ebene wird seit rund zwei Jahren durch ein umfangreiches Gesetzespaket ausgebaut. Das geforderte Tempo ist jedoch ein Problem, denn die Kommission muss die Rechtspolitiken sämtlicher 28 Mitgliedstaaten harmonisieren. 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«[44], im Klartext also eine protektionistische Politik.

4.3 Zivilität

Es gilt der Versuchung zu widerstehen, auf die wachsende Zahl digitaler Angriffe mit dem Aufbau einer digitalen Rüstungsindustrie und damit Cyber-Offensivwaffen zu reagieren. Die Verteidigungspolitischen Richtlinien vom Mai 2011 enthalten bereits die Vorgabe, dass die deutschen Streitkräfte ein möglichst breites Fähigkeitsspektrum abdecken müssen. Militärisch wird der Informationsraum im neuen Weißbuch der Bundesregierung 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«.[45] Derartige Formulierungen und Strategieentscheidungen bergen die Gefahr, dass der Cyberraum versicherheitlicht oder gar militarisiert wird und so eine neue Proliferation von Cyberwaffen entsteht.

5. Fazit

Der Cyber-Außen- und Sicherheitspolitik ist ein weites Sicherheitsverständnis zugrunde zu legen. Das wiederum heißt, dass alle Beteiligten in Staat, Wissenschaft, Wirtschaft und Gesellschaft gemeinsam ihre Verantwortung zur Cybersicherheit wahrnehmen müssen. „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 – das jedenfalls ist eine der zentralen Erkenntnisse des Sicherheitsforschungsprogramms des BMBF."[46] Wenn die Bundeswehr wie geplant 13.500 Soldaten für die Cyberabwehr vorhalten will, stellt sie sich damit neben den Dimensionen Land, See, Luft und Weltall auch im Cyberraum als Operationsgebiet für die deutschen Streitkräfte auf. Im aktuellen Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr" heißt es, dass sich die Bundeswehr für den Umgang mit komplexen Angriffen aufstellen müsse: „Die Verteidigung gegen derartige Angriffe bedarf auch entsprechender defensiver und offensiver Hochwertfähigkeiten, die es kontinuierlich zu beüben und weiterzuentwickeln gilt." Sicher sollte das Militär eine Rolle in der Cyberverteidigung spielen, es ist aber nur ein Akteur unter vielen bei der Lösung einer gesamtgesellschaftlichen Aufgabe. Ganz besonders in Friedenszeiten sollte es darum gehen, ausschließlich die zivile Cybersicherheit und -abwehr zu stärken, und im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU und in der Nato sind diese Hochwertfähigkeiten abzustimmen. Insbesondere ist in kostenintensive Hochsicherheitstechnologie zu investieren. Ein freies Internet braucht Vertrauen, und das kann man nicht durch militärische oder sonstige Zwangsmaßnahmen erzeugen. Das gilt für die digitale wie für die analoge Welt. Um Vertrauen aufzubauen, benötigt die Politik eine gemeinsame Idee von der Gestaltung des Informations- und bzw. Cyberraums. Hier scheint mir die völkerrechtliche Norm der Sorgfaltsverantwortung hilfreich, die besagt, dass in Friedenszeiten keine Handlungen vom eigenen Territorium ausgehen dürfen, die die Rechte anderer Staaten verletzen. Solange die Durchsetzung dieser Norm international nicht gelingt, sollte man sich zumindest national und möglichst auch europäisch bzw. transatlantisch auf diese gemeinsame Idee verpflichten.

Dr. **Annegret Bendiek** ist Wissenschaftlerin am Deutschen Institut für Internationale Politik und Sicherheit der Stiftung für Wissenschaft und Politik. 2015 war sie Projektleiterin des Projekts »Die Herausforderung der Digitalisierung für die deutsche Außen- und Sicherheitspolitik«.

41 *CDU, CSU* und *SPD*, Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode, Dezember 2013, http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile (abgerufen am 16.9.2016).

42 *CDU, CSU* und *SPD*, Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode [wie Fn. 35], S. 147.

43 *Europäische Kommission*, Strategie für einen digitalen Binnenmarkt für Europa, Mai 2015, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=DE (abgerufen am 16.9.2016).

44 *Ansgar Baums*, Der weiße Elefant: Industriepolitik durch die Hintertür des Datenschutzes?, 10.03.2015, http://plattform-maerkte.de/der-weisse-elefant-industriepolitik-durch-die-hintertuer-des-datenschutzes/ (abgerufen unter 16.9.2016).

45 Andre Meister, Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe [wie Fn. 18].

46 *Christopher Daase*: Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik, Vortrag zum SWP-CyberLab im September 2015.