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

Annegret Bendiek

Europäische Cybersicherheitspolitik

S 15
Juli 2012
Berlin

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

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

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

Dr. Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU-Außenbeziehungen

Europäische Cybersicherheitspolitik

Sicherheitspolitik ist in einem grundlegenden Wandel begriffen. Die Territorialverteidigung gegen Panzerarmeen hat ihren einst zentralen Stellenwert in Europa großteils eingebüßt. Immer bedrohlicher dagegen werden unter anderem unsichtbare, räumlich kaum noch identifizierbare Gegner. Virtuelle Angriffe auf kritische Infrastrukturen, Regierungsinstitutionen und die individuelle Datensicherheit fordern die Sicherheitspolitik im 21. Jahrhundert immer stärker heraus. Außerordentlich wichtig ist ein sicheres Internet aber auch für die Freiheit des Einzelnen, für informationelle Selbstbestimmung und damit für die Demokratie selbst.

Die sich allmählich entwickelnde europäische Cybersicherheitspolitik soll helfen, vereinbarte Mindeststandards in allen ihren Mitgliedstaaten umzusetzen, und zwar bei Prävention, Abwehrbereitschaft (resilience), Reaktion und internationaler Kooperation. Sie soll nationale Sicherheit befördern, jedoch ohne gegen demokratische Grundprinzipien zu verstoßen und die individuellen Freiheiten über Gebühr zu beschränken. Es ist nicht leicht, beides miteinander in Einklang zu bringen. Daher stellt sich die Frage nach den demokratiepolitischen Implikationen europäischer Cybersicherheitspolitik. Wie verhalten sich deren institutionelle Strukturen und Instrumente zu den Anforderungen demokratischen Regierens? Um dies zu klären, werden zunächst die wesentlichen Herausforderungen für das Bemühen um mehr Sicherheit im Internet skizziert. Daraufhin wird die institutionelle Architektur der globalen Cybersicherheitspolitik umrissen, und die wichtigsten Organisationsprinzipien europäischer Cyberpolitik werden identifiziert. Schließlich wird bewertet, inwieweit diese Architektur mit demokratischen Prinzipien vereinbar ist, und es werden Vorschläge diskutiert, wie mehr Sicherheit im Internet herzustellen wäre, ohne jene zu verletzen. Nicht berücksichtigt werden militärische und völkerrechtliche Aspekte des Datenraums, die notwendigen technischen Mittel einer Internetregulierung oder die innenpolitischen Diskurse in EU-Mitgliedstaaten.

Es lohnt sich, die EU genauer unter die Lupe zu nehmen, denn sie ist ein institutionelles Laboratorium, in dem heute das ausprobiert wird, was morgen auf der internationalen Ebene umgesetzt werden

könnte. Ähnlich wie die EU-Strategie zur Terrorismusbekämpfung kann die geplante EU-Strategie zur Cybersicherheit daher als Scharnier zur internationalen Regulierung und als Instrument innereuropäischer Koordinierung wirken. Auf EU-Ebene zeigt sich, was und wie künftig global reguliert werden könnte.

Die europäische Cybersicherheitspolitik ist auf vielfältige Weise sowohl in internationale als auch innerstaatliche Regelungszusammenhänge eingebunden. Sie wird im Kontext einer globalen Mehrebenen- und Multistakeholder-Struktur formuliert und interpretiert. Dabei offenbaren sich drei zentrale demokratiepraktische Probleme:

Verschmelzung innerer und äußerer Politik: Diese Bereiche lassen sich in der europäischen Sicherheitspolitik kaum noch trennen. Internetbasierte Angriffe auf wichtige Infrastrukturen des Staates können aus Ghana, aus Russland oder aus der Wohnung gegenüber kommen. Oftmals ist es nur noch sehr schwer oder gar nicht mehr möglich, die Herkunftsorte von Gefahrenquellen zu ermitteln. Aus diesem Grund verschwimmen die Zuständigkeitsbereiche der Innen- und der Außenpolitik, so dass sicherheitspolitische Herausforderungen sich kaum mehr eindeutig zuordnen lassen. In der Praxis zeigt sich diese Schwierigkeit in einer sektorübergreifenden Kooperation unterschiedlichster Behörden und Gewalten. Diese Vermischung traditioneller Rollen in der Problembearbeitung ist in der EU noch komplizierter als in einzelnen Staaten, aber keineswegs neu. In den letzten Jahren wird die Entwicklung europäischer Sicherheitspolitik maßgeblich von einer Internationalisierung der Innen- und Justizpolitik bestimmt, während die politische Bedeutung der GASP in der Cybersicherheitspolitik sich im Handeln der dominanten fünf Mitgliedstaaten (Deutschland, Frankreich, Großbritannien, Niederlande, Schweden) konzentriert. Die Europäische Kommission und das Europäische Parlament erhalten hier völlig neue Gestaltungsmöglichkeiten.

Versicherheitlichung: Einst hatte die EU das Ziel, einen gemeinsamen »Raum der Freiheit, der Sicherheit und des Rechts« aufzubauen. Unter dem Eindruck der neuen Bedrohungslagen interpretieren Mitgliedstaaten und Kommission dies jedoch zunehmend einseitig zugunsten sicherheitspolitischer Maßnahmen. Die politische Schwerpunktsetzung verschiebt sich von der Freiheit zur Sicherheit. Private Sicherheitsunternehmen üben immer mehr Einfluss auf diesen Politikbereich aus.

Privatisierung von Regieren: Auch die Trennung zwischen privat und öffentlich verliert in den neuen politischen Strukturen dramatisch an Bedeutung. Ohne technologisches Know-how aus Unternehmen lassen sich weder die relevanten Gefahren angemessen identifizieren noch sinnvolle Antworten formulieren. Zahlreiche private Unternehmen bestimmen die Daseinsvorsorge in Energie, Gesundheit oder Verkehr und bilden damit strategisch wichtige Infrastrukturen des Staates. Ihre Einbindung in die Identifikation von Bedrohungen sowie das Risiko- und Krisenmanagement ist ausschlaggebend für die öffentliche Sicherheit. Garantiert wird diese von den Behörden, die den verfassungsmäßigen Auftrag dafür erhalten haben.

Um die institutionellen Strukturen und Instrumente der europäischen Cybersicherheitspolitik in Einklang mit den Anforderungen demokratischen Regierens zu bringen, lassen sich folgende Leitlinien formulieren: »Gutes Regieren« in der europäischen Cybersicherheitspolitik sollte sich an Kriterien wie Transparenz, Rechtsstaatlichkeit, Rechenschaftspflicht und Partizipation messen lassen. Zu betonen ist die konstruktive Rolle der Parlamente bei der institutionellen und materiellen Regulierung der Cybersicherheitspolitik. Sie übernehmen eine wichtige Funktion, nämlich die Kommunikation mit der Öffentlichkeit. In demokratischen Strukturen sollten Parlamente der Ort sein, an dem das Verhältnis von Sicherheit und Freiheit definiert wird, gerade auch was Cybersicherheitspolitik anbelangt. Die Verhandlungen über das Internationale Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA) haben vorgeführt, dass es nicht der Sache dient, intransparente, nicht öffentlich debattierte und exklusive Politik zu betreiben. Nichtstaatliche Gruppen wie Vertreter der Internetwirtschaft, der Zivilgesellschaft und der technischen Community sollten konsequent in politische Entscheidungsprozesse einbezogen werden. Auf diese Weise würde europäische Koordinierung den Prinzipien der gewachsenen Internetkultur folgen. Sie wäre »open« statt »closed«, »bottom up« statt »top down« und »inklusiv« statt »exklusiv«.

Herausforderungen für Markt und Staat

Ein wesentliches Problem besteht darin, dass es keinerlei systematische quantitative Erfassung von Sicherheitsbedrohungen im Internet gibt.[1] Es existiert weder eine nationale noch eine internationale Institution, die über die technischen Möglichkeiten oder die rechtlichen Kompetenzen verfügt, alle internetbasierten Angriffe auf Unternehmen, Regierungsstellen und private Accounts zu registrieren.[2] Wer Bedrohungen der Internetsicherheit beschreiben will, muss sich daher weitgehend auf Berichte von Experten und Regierungsstellen verlassen.[3]

Cybersicherheit wird in diesen Berichten oftmals in drei Bereiche unterteilt: Cyberkriminalität, Cyberspionage und Cyberwar.[4] International anerkannte Definitionen dieser drei Begriffe gibt es bisher allerdings nicht. Grundsätzlich aber kann man Cyberkriminalität als Verstöße gegen Eigentumsrechte nichtstaatlicher Akteure bezeichnen, zum Beispiel Phishing.[5] Cyberspionage umfasst Einbrüche in die Datenbanken staatlicher oder nichtstaatlicher Unternehmen durch fremde Regierungsbehörden. Unter Cyberwar werden Versuche eines Staates verstanden, einen anderen Staat mit Hilfe des Internets nachhaltig zu schädigen. Doch keine dieser Arbeitsdefinitionen ist eindeutig und klar abgrenzbar.[6] Nirgendwo ist politisch und rechtlich unmissverständlich und allgemeinverbindlich definiert, wo die Grenzen zwischen Cyberkriminalität, Cyberspionage und Cyberwar verlaufen. Genauso wenig ist festgelegt, welche Tatmerkmale erfüllt sein müssen, um Handlungen entsprechend einordnen zu können.[7]

Die Schwierigkeiten, die einer internationalen Einigung auf gemeinsame Definitionen und Tatbestandsmerkmale entgegenstehen, sind nicht nur Ausdruck eines Streits über technische und juristische Feinheiten. Sie offenbaren ein grundlegend divergierendes Problemverständnis bezüglich Notwendigkeit und angemessener Reichweite staatlicher Regulierungen.[8]

1 Siehe zur Szenarienbildung in der Cybersicherheitspolitik Sacha Tessier Stall, *The Future of Cybersecurity*, Den Haag: The Hague Centre for Strategic Studies and TNO, 2011. Zur Systematik des Cyberspace und Sicherheit siehe die Studie von Shmuel Even/David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv: Institute for National Security Studies, Mai 2012.

2 Der Aktionsplan zur Umsetzung des Stockholmer Programms sieht zwar die Einführung eines Observatory for the Prevention of Crime (OPC) vor. Dieses soll seine Arbeit allerdings erst 2013 aufnehmen. Vgl. David Brown, »The Stockholm Solution? Papering over the Cracks within the Area of Freedom, Security and Justice«, in: *European Security*, 20 (Dezember 2011) 4, S. 481–503.

3 Beispiele hierfür sind die Liste der einschlägigen Cyberattacken 2010 bei Alexander Klimburg/Heli Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, Studie im Auftrag des Europäischen Parlaments, PE 433.828, Brüssel, April 2011, S. 54, oder der Beitrag von Myriam Dunn Cavelty, »The Militarisation of Cyber Security as a Source of Global Tension«, in: Daniel Möckli (Hg.), *Strategic Trends 2012: Key Developments in Global Affairs*, Zürich: Center for Strategic Studies (CSS), ETH Zürich, 2012, S. 103–124.

4 In der Literatur werden auch die folgenden vier Kategorien unterschieden: »Cyberwar – Warfare in cyberspace. This includes warfare attacks against a nation's military – forcing critical communications channels to fail, for example – and attacks against the civilian population. Cyberterrorism – The use of cyberspace to commit terrorist acts. An example might be hacking into a computer system to cause a nuclear power plant to melt down, a dam to open, or two airplanes to collide. [...] Cybercrime – Crime in cyberspace. This includes much of what we've already experienced: theft of intellectual property, extortion based on the threat of DDOS attacks, fraud based on identity theft, and so on. Cybervandalism – The script kiddies who deface websites for fun are technically criminals, but I think of them more as vandals or hooligans«. Bruce Schneier, *Schneier on Security* (Blog), <http://www.schneier.com/blog/archives/2007/06/cyberwar.html> (eingesehen am 22.3.2012).

5 Phishing ist der Versuch, bei der elektronischen Kommunikation auf betrügerische Weise an sensible Daten wie Passwörter oder Kreditkarteninformationen zu gelangen. Dabei geben sich die Täter als vertrauenswürdige Personen aus.

6 Als Beispiel für den Bereich der Cyberkriminalität siehe die Studie von Neil Robinson u.a., *Feasibility Study for a European Cybercrime Centre*. Prepared by RAND Europe for the European Commission, Brüssel 2012, S. 17–55.

7 Vgl. Alexander Klimburg, »Mobilising Cyber Power«, in: *Survival*, 53 (Februar–März 2011) 1, S. 41–60; Friedrich Wilhelm Kriesel/David Kriesel, »Cyberwar – relevant für Sicherheit und Gesellschaft? Eine Problemanalyse«, in: *Zeitschrift für Außen- und Sicherheitspolitik*, 5 (2011) 4, S. 205–216 (214).

8 Laut Kleinwächter »spielen bei der Regulierung des Internet drei Layer [Ebenen, d. Verf.] eine Rolle: der Transport-Layer – das ist im Wesentlichen die Telekommunikations-

Manche möchten eine zentralisierte zwischenstaatliche Organisation mit umfassender Kompetenz für die Regulierung des Internets etablieren. Andere wiederum wollen das dezentral funktionierende Multistakeholder-Governance-Modell weiterentwickeln, bei dem Regierungen, Privatwirtschaft, Zivilgesellschaft und technische Community in ihren jeweiligen Rollen gleichberechtigt zusammenarbeiten, und die Selbstregulierungskräfte und wechselseitigen Verantwortlichkeiten aller Betroffenen und Beteiligten stärken.[9] Beispiele für die teilweise sehr grundsätzlich geführten Debatten sind die Auseinandersetzungen über die Wikileaks-Affäre, ACTA[10] und aktuell die Datenvorratsspeicherung.

In allen drei Fällen sind sowohl zwischenstaatliche als auch innerstaatliche Streitigkeiten zu beobachten, die sich um die Grenzen legitimer staatlicher Interventionen und die zu respektierenden Freiheitsrechte des Einzelnen drehen. Im Wikileaks-Fall stuften die US-Behörden die Veröffentlichung von Regierungsdokumenten als schweres Verbrechen ein und sorgten dafür, dass Wikileaks seine Stammadresse ».org« verlor. Verbote in der Schweiz und Schweden folgten kurz danach. Gegner dieses Vorgehens argumentieren, Wikileaks sei angemessener als neue Art neutrales Trägermedium zu behandeln und dürfe nicht dafür bestraft werden, wie und von wem es benutzt werde.[11] ACTA gilt wirtschaftsnahen Kreisen als notwendiges Instrument zum Schutz geistigen Eigentums, während die überwiegende Mehrzahl der privaten Internetnutzer und -aktivisten staatliche Maßnahmen in diesem Bereich eher als Bedrohung ihrer Freiheit im Netz sehen.[12] Ähnlich stoßen auch die Versuche der EU, eine allgemeine Richtlinie zur Datenvorratsspeicherung durchzusetzen, in Deutschland auf heftigen Widerstand. Die vom Bundestag vorgesehenen Umsetzungsmaßnahmen wies das Bundesverfassungsgericht mit der Begründung zurück, es handle sich hier um einen übermäßigen Eingriff in das Post- und Fernmeldegeheimnis (siehe unten, Abschnitt »Versicherheitlichung«).

In Anbetracht dieser Unklarheiten ist es wenig sinnvoll, mit den Begriffen Kriminalität, Spionage und Kriegführung zu arbeiten. Stattdessen empfiehlt es sich, zwischen Herausforderungen der nationalen Sicherheit einerseits und Gefahren für die Funktionsweise des marktwirtschaftlichen Systems sowie für privates Eigentum andererseits zu unterscheiden.

Gefährdungen privaten Eigentums

Das Internet ermöglicht eine Vielzahl neuer krimineller Handlungen, die sich auf die Aneignung des Eigentums anderer richten.[13] Mit Hilfe von Instrumenten wie Identitätsdiebstahl, Phishing, Spams und bösartigen Codes können groß angelegte Betrugsdelikte verübt werden.[14] Der Schaden aus Betrugsstraftaten

infrastruktur, die durch nationales Telekommunikationsrecht und internationale Abkommen im Rahmen der ITU geregelt ist; der Protokoll-Layer – im engeren Sinn ›das Internet‹ mit seinen Codes, Standards, Protokollen, dem IP-Adress- und Domainnamensystem –, der von nichtstaatlichen globalen Institutionen wie der Internet Engineering Task Force (IETF), dem World Wide Web Consortium (W3C), des Institute of Electrical and Electronics Engineers (IEEE), der Internet Corporation for Assigned Names and Numbers (ICANN) oder den Regional Internet Registries (RIRs) geregelt wird; der Anwendungs-Layer – das sind all die Dienste, die über das Internet laufen, von eCommerce bis zu den sozialen Netzwerken, die gleichfalls primär durch nationales Recht und dabei sogar weitgehend durch Verfassungsrecht wie Meinungsäußerungsfreiheit oder Schutz von Eigentum und Privatsphäre geregelt sind.« Wolfgang Kleinwächter, »Wie reguliert man den Cyberspace? Die Quadratur des Dreiecks«, in: *Heise Online – Telepolis*, 29.5.2012, <http://www.heise.de/tp/druck/mb/artikel/34/34742/1.html> (eingesehen am 2.6.2012; Fehler im Originaltext wurden korrigiert, d. Verf.).

9 Vgl. Wolfgang Kleinwächter, »Kalter Krieg im Cyberspace oder konstruktiver Dialog? Ausblick auf die Internetpolitik 2012«, in: *Heise Online – Telepolis*, 20.1.2012, <http://www.heise.de/tp/druck/mb/artikel/36/36266/1.html> (eingesehen am 17.3.2012).

10 Siehe hierzu die EP-Studie zu ACTA: *The Anti-Counterfeiting Trade Agreement (ACTA): an Assessment*, Studie im Auftrag des Europäischen Parlaments, PE 433.859, Brüssel 2011.

11 Vgl. Geert Lovink/Patrice Riemens, »Die Anarchie der Transparenz«, in: *Frankfurter Rundschau*, 7.12.2010, S. 32; siehe auch François Heisbourg, »Leaks and Lessons«, in: *Survival*, 53 (Februar–März 2011) 1, S. 207–216.

12 Eine sehr gelungene Darstellung der unterschiedlichen Positionen zum Thema findet sich in »Acta-Exegese: Ist es nun das Ende des freien Internet oder nicht?«, in: *Frankfurter Allgemeine Zeitung* (online), 23.2.2012, <http://www.faz.net/aktuell/feuilleton/medien/acta-exegese-ist-es-nun-das-ende-des-freien-internet-oder-nicht-11660030.html> (eingesehen am 23.2.2012).

13 Unter Internetkriminalität versteht die EU-Kommission alle kriminellen Handlungen, »die mittels elektronischer Kommunikationsnetze und Informationssysteme begangen oder gegen derartige Netze und Systeme verübt werden«. Europäische Kommission, *Mitteilung der Kommission: Eine allgemeine Politik zur Bekämpfung der Internetkriminalität*, KOM (2007) 267 endg., Brüssel, 22.5.2007.

14 Die Bedrohungen lassen sich laut EU-Kommission in folgenden Kategorien zusammenfassen: »*kriminelle Ausnutzung*, z.B. durch ›komplexe anhaltende Angriffe‹ (advanced persis-

im Zusammenhang mit Online-Banking, Identitätsdiebstahl und Kreditkartenbetrug steigt rasant. Laut der deutschen polizeilichen Kriminalstatistik wurden hierzulande im Jahr 2008 rund 38 000 Straffälle gemeldet. Im Jahr 2010 dagegen waren es schon rund 60 000 Meldungen, und die Schäden summierten sich auf 60 Millionen Euro.[15]

In einer aktuellen Studie des IT-Sicherheitsunternehmens McAfee sind 36 Prozent aller befragten Wirtschaftsführer, Wissenschaftler und politischen Entscheidungsträger aus 27 europäischen Ländern der Auffassung, dass die Abwehr von Cyberangriffen auf kritische Infrastrukturen (etwa Stromversorger, Banken, Versicherungen, Transport) genauso wichtig ist wie die Raketenabwehr.[16] Weiterhin berichten 43 Prozent der Befragten, dass sie schon einmal Schäden in der kritischen Infrastruktur beklagen mussten, die von Hackern verursacht worden waren. In der Studie des Vorjahres waren es nur 37 Prozent.[17] Auch der Cyber Security Risks Report, verfasst von den Digital Vaccine Laboratories (DVLabs) der Firma Hewlett-Packard, unterstreicht diesen Trend.[18] Demnach waren im ersten Halbjahr 2011 65 Prozent mehr Angriffe auf Webanwendungen zu verzeichnen als im ersten Halbjahr 2010. Außerdem werden die Attacken immer komplexer und untergraben deshalb bei einem Großteil der Befragten das Vertrauen in die eigene IT-Sicherheit. Weniger als 30 Prozent aller Führungskräfte sind überzeugt, dass ihre IT-Systeme gut vor Angriffen geschützt sind.

Nach Angaben der EU-Kommission werden täglich eine Million Menschen Opfer von Internetkriminalität.[19] Dazu zählen auch Spam-Mails und elektronische Post von Betrügern, die nach Kontodaten fragen. Illegale Machenschaften machen es möglich, dass Kreditkartendaten für gerade einmal einen Euro pro Karte zu kaufen sind. Eine gefälschte Kreditkarte wird unter organisierten Kriminellen für rund 140 Euro gehandelt, Bankkontendaten für lediglich 60 Euro. Jeden Tag werden bis zu 600 000 Facebook-Konten gesperrt, weil Hacker versuchen, auf sie zuzugreifen. Allein im Jahr 2009 wurden über 6,7 Millionen mit Bots infizierte Computer ermittelt.[20]

Nach Schätzung von McAfee erleiden US-amerikanische und europäische Unternehmen durch Wirtschaftsspionage jedes Jahr Schäden von insgesamt einer Billion Dollar in Form entgangener Geschäfte, wertloser Ausgaben für Forschung und Entwicklung und zusätzlicher Aufwendungen zur Abwehr von Cyberattacken. Vorfälle wie bei Sony und Adidas verdeutlichen zudem, dass IT-Angriffe Firmen nicht nur wirtschaftlich beeinträchtigen, sondern auch deren Image beschädigen können. Im April 2011 war es Unbekannten gelungen, sich Zugang zu Informationen über mehr als 100 Millionen Kunden von Onlinediensten des japanischen Elektronikkonzerns Sony zu verschaffen. Der Sportartikelkonzern Adidas war im November 2011 Zielscheibe eines Hackerangriffs. Um Daten von Kunden zu schützen, sperrte die Firma ihre Internetseite.

Wie massiv geistiges Eigentum gefährdet ist, zeigen Schätzungen, denen zufolge es etwa 30 000 Schwachstellenanalytiker gibt, die betroffenen Herstellern oder der global operierenden organisierten IT-Kriminalität ihre Erkenntnisse über Einbruchs- und Manipulationsmöglichkeiten von IT-Systemen verkaufen.[21] Was das

tent threats, APT) zur wirtschaftlichen oder politischen Spionage (z.B. GhostNet), Identitätsdiebstahl, die jüngsten Angriffe auf das Emissionshandelssystem oder Angriffe auf staatliche IT-Systeme; *Störung*, wie durch DDoS-Angriffe (Distributed Denial of Service – koordinierte Überlastungsangriffe auf Server) oder Spamming über Botnetze (z.B. das Conficker-Netz mit 7 Millionen Computern und das von Spanien ausgehende Mariposa-Netz mit 12,7 Millionen Computern), Stuxnet sowie das Unterbinden der Kommunikation über bestimmte Kommunikationsmittel; *Zerstörung*. Dieses Szenario wurde noch nicht verwirklicht, kann jedoch angesichts der immer stärkeren Durchdringung kritischer Infrastrukturen mit IKT [Informations- und Kommunikationstechnologie, d. Verf.] (z.B. intelligente Netze und Wasserversorgungssysteme) in Zukunft nicht ausgeschlossen werden.« Siehe Europäische Kommission, *Mitteilung der Kommission über den Schutz kritischer Infrastrukturen. Ergebnisse und Schritte: der Weg zur globalen Netzsicherheit*, KOM(2011) 163 endg., 31.3.2011, S. 4.

15 Vgl. Bundeskriminalamt, *Cybercrime: Bundeslagebild 2010*, <http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true> (Zugriff am 21.6.2012), S. 6.; vgl. aktuell »Cyber Criminals Steal Millions from EU Banks«, in: *EUObserver*, 27.6.2012.

16 Vgl. Brigid Grauman, *Cybersecurity: the Vexed Question of Global Rules,* Brüssel: Security and Defence Agenda, Februar 2012.

17 Vgl. Jens Koenen, »Das Wettrüsten für den Cyber-War ist in vollem Gange«, in: *Handelsblatt*, 31.1.2012, S. 23.

18 Vgl. Hewlett-Packard DVLabs (Hg.), *Secure Your Network. 2010 Full Year Top Cyber Security Risks Report*, März 2011.

19 Die Daten basieren auf einer Pressemitteilung der Europäischen Kommission, *EU-Zentrum zur Bekämpfung der Cyberkriminalität und zum Verbraucherschutz beim elektronischen Geschäftsverkehr*, IP/12/317, Brüssel, 28.3.2012.

20 Vgl. ebd. Bots oder Botnets (Kurzform von Roboternetzwerk) sind Netzwerke infizierter Rechner, die ferngesteuert werden können, um einen koordinierten Angriff auszuführen.

21 Michael Spehr, »Angriff auf IT-Systeme: Das Spiel der

Ausspionieren privater Unternehmensdaten anbelangt, sind der europäische Binnenmarkt und vor allem Deutschland in den letzten Jahren zu bevorzugten Angriffszielen für Internetkriminalität geworden. Nach Auffassung der Bundesregierung[22] und hochrangiger Wirtschaftsvertreter[23] ist sich die mittelständische Wirtschaft jedoch noch nicht hinreichend bewusst, welche Risiken ungewollte Know-how-Abflüsse mit sich bringen. Dieses mangelnde Bewusstsein steht in scharfem Kontrast zur hohen Relevanz, die Fragen der Cybersicherheit für alle hochentwickelten Dienstleistungsgesellschaften und damit für alle EU-Staaten haben. Moderne Dienstleistungsgesellschaften zeichnen sich durch komplexe und vernetzte Produktionsweisen aus. Sichere internetbasierte Kommunikationsinfrastrukturen und ein effektiver Schutz geistigen Eigentums sind dafür notwendige Vorbedingungen. Ohne sichere Kommunikationsmodi ist es nicht möglich, die unterschiedlichen Produktionsphasen angemessen zu organisieren, Wissen zu koordinieren und Produktionsketten zu strukturieren. Wesentliche Bereiche der Daseinsvorsorge und der staatlichen Infrastruktur sind zudem an das Internet gekoppelt und damit hochgradig verwundbar gegenüber Angriffen durch schädliche Software (Malware).[24]

Gefahren für die staatliche Sicherheit

Die staatliche Sicherheit ist durch das Internet ebenfalls auf mannigfache Weise gefährdet. Seit 2005 werden vermehrt zielgerichtete Angriffe sowohl auf Bundesbehörden als auch auf die Industrie beobachtet, die mit Hilfe von Spionagetrojanern ausgeführt wurden.[25] Der damalige Innenminister Thomas de Maizière berichtete auf der Münchner Sicherheitskonferenz 2011, dass das deutsche Regierungsnetz pro Tag vier- bis fünfmal unter Beteiligung fremder Nachrichtendienste attackiert werde.[26] Cyberspionage wird auch dadurch gefährlicher, dass eine Reihe von Staaten Cyberangriffe als Mittel zur Informationsbeschaffung einsetzen.[27] Auch deutsche Behörden versuchen offensichtlich auf diese Weise gezielt Daten anderer Staaten zu erheben. So soll der Bundesnachrichtendienst (BND) in 90 Fällen Computer in Afghanistan und im Kongo infiltriert haben.[28] Immer häufiger arbeiten Staaten dabei mit privaten Hackergruppen zusammen, die für sie in private Datenbanken einbrechen, um an strategisch wichtiges Unternehmenswissen zu gelangen. Experten gehen davon aus, dass es mehrere hundert Millionen Schadprogramme und über 100 Organisationen gibt, die an anspruchsvollen militärischen, geheimdienstlichen oder terroristischen Cyberoperationen mitwirken.[29]

All diese Aktionen werden häufig unter dem Begriff Cyberkrieg zusammengefasst.[30] In einer weiten Interpretation lassen sich hierunter all diejenigen Handlungen eines Staates gegenüber einem anderen fassen, bei denen internetbasierte Instrumente genutzt

Hacker«, in: *Frankfurter Allgemeine Zeitung*, 11.5.2011.

22 Interview mit Bundesinnenminister Hans-Peter Friedrich, »›Cyberangriffe werden weiter zunehmen‹«, in: *Handelsblatt*, 3.2.2012, S. 17.

23 So »könne ein einziger Mitarbeiter mit dem entsprechenden Zugang das gesamte Wissen eines Unternehmens innerhalb weniger Minuten auf einen USB-Stick kopieren und weitergeben. [...] die meisten Informationen werden immer noch von Menschen verbreitet. [...] ›Eine einheitliche Unternehmenskultur und klare ethische Richtlinien bieten weiteren Schutz‹, so Wiedemann.« Siehe »Daimler-Sicherheitschefin Sabine Wiedemann referiert über Wirtschafts- und Industriespionage beim Neujahrsempfang des CDU-Kreisverbandes Enzkreis/Pforzheim«, *Website von CDU-MdB Gunther Krichbaum*, <http://www.gunther-krichbaum.de/nc/startseite/aktuell/artikel/daimler-sicherheitschefin-sabine-wiedemann-referiert-ueber-wirtschafts-und-industriespionage-beim-n.html> (eingesehen am 30.3.2012).

24 Eine Übersicht über die nationalen Politiken zum Schutz kritischer Infrastrukturen bieten Elgin M. Brunner/Manuel Suter, *International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Zürich: CSS, 2008.

25 Siehe Deutscher Bundestag, *Kleine Anfrage der Abgeordneten Jan Korte u.a.: Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage (»Staatstrojaner«)*, Drucksache 17/7104, 25.10.2011.

26 Vgl. Paul-Anton Krüger, »Wettrüsten im virtuellen Raum«, in: *Süddeutsche Zeitung*, 7.2.2011; Jens Koenen u.a., »Der Verteidigungsfall im Netz. Computerviren in der Hand von Terroristen«, in: *Handelsblatt*, 27.1.2012, S. 21.

27 Siehe hierzu ausführlich Klimburg, »Mobilising Cyber Power« [wie Fn. 7].

28 So Hubert Gude, »Geheimdienst: Trojaner im Dienst«, in: *Focus*, 23.3.2009.

29 Daten nach Peter W. Singer, »Schlachtfelder der Zukunft«, in: *Süddeutsche Zeitung*, 4.2.2011.

30 Folgende Autoren sprechen ausdrücklich von Cyberwar: Richard A. Clarke/Robert K. Knake, *World Wide War. Angriff aus dem Internet*, Hamburg 2011; Sandro Gaycken, *Cyberwar. Das Internet als Kriegsschauplatz*, München 2010; ders., *Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand*, München 2012.

werden, um den anderen Staat zu schädigen.[31] Auf die Frage, ob wir im Cyberkrieg leben, antwortete Michael Hayden, ehemals Leiter des amerikanischen Auslandsgeheimdienstes Central Intelligence Agency (CIA): »Das kommt auf die Definition an. Sicher ist, es gibt einen Machtkampf der Nationen im Netz. Aber das meiste davon ist Spionage, kein Krieg.«[32] Cyberkrieg kann mit Hilfe eingeschleuster Würmer oder breit angelegter Angriffe durch sogenannte Botnets geführt werden. Im Jahr 2007 wurde ein massiver Botnet-Angriff auf Estland gestartet. Zahllose Computer wurden infiziert und miteinander koordiniert und überschütteten estnische Regierungsserver so lange mit Anfragen, bis diese vom Netz genommen werden mussten. Im März 2009 griff ein Netz manipulierter Rechner die Computersysteme staatlicher und privater Organisationen in über 100 Ländern an und verschaffte den Hackern Zugang zu sensiblen und vertraulichen Dokumenten.[33] Ähnliche Angriffe hatte es schon 2004 auf Malta und 2008 auf Georgien gegeben.

Der Einsatz des im Juli 2010 publik gewordenen Malwareprogramms Stuxnet ist der inzwischen wohl bekannteste Fall eines Angriffs auf Einrichtungen eines anderen Staates. Vermutet wird, dass es Israel und die USA waren, die auf diese Weise Iran schaden wollten.[34] Komplexität, Wirkungsweise und Angriffsziel dieses Computervirus lassen auf höchste Professionalität mit den entsprechenden personellen und finanziellen Ressourcen schließen. Stuxnet wird wahrscheinlich kein Einzelfall bleiben, sondern eine Vielzahl von Nachahmern finden. Weltweit sollen derzeit an die 100 staatliche und nichtstaatliche Expertenteams damit beschäftigt sein, Software und Wirkungsweise von Stuxnet zu kopieren und eigene Malware für Attacken auf missliebige Infrastrukturen zu konstruieren.[35] Im Mai 2012 haben IT-Experten einen neuen Computerschädling identifiziert. Das Virus, bekannt als Flame, Flamer oder Skywiper, sei mindestens seit August 2010 im Einsatz und wahrscheinlich von einem Staat initiiert worden. Tausende Rechner vor allem im Nahen Osten sollen infiziert sein. Zwar verursacht das Virus keine physischen Schäden, kann aber riesige Mengen sensibler Daten sammeln. Spekulationen darüber, dass die Schadsoftware aus israelischer Produktion stamme, wurden nie offiziell dementiert.[36] Stuxnet und Flame sind Lehrbuchbeispiele für »die janusköpfige Natur der Forschung an Sicherheitslücken«[37] und eindrückliche Nachweise für die neuen Offensivfähigkeiten, die sich viele Staaten zulegen.

Das US Cyber Command, eine Stabsstelle der digitalen Landesverteidigung, verfügt inzwischen über 90 000 Mitarbeiter und einen Etat von rund 3 Milliarden Dollar. Die Cyberwar-Einheiten der US-Armee rühmen sich nicht erst seit heute, sie seien in der Lage, durch Internetangriffe den Strom in jeder beliebigen Stadt der Welt abzuschalten.[38] Im Fall kriegerischer Auseinandersetzungen kann die elektronische Kampfführung mit Mitteln der Informationstechnik eine Schlüsselrolle spielen. Die hochtechnisierten Formen des Krieges im Informationszeitalter basieren auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischen Fähigkeiten. Daher ist es unter Globalisierungsbedingungen eher unwahrscheinlich, dass sich das Kriegsgeschehen auf das Gefechtsfeld kriegführender Nationen begrenzen wird. »Der Cyberwar ermöglicht eine gewisse Rückkehr des Krieges, trotz der Unmöglichkeit großer konventioneller Konflikte.«[39]

31 Siehe Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Washington, D.C.: Atlantic Council of the United States, Januar 2012; zur juristischen Heranführung Eneken Tikk, »Ten Rules for Cyber Security«, in: *Survival*, 53 (Juni–Juli 2011) 3, S. 119–132; zur strategischen Debatte Paul Cornish u.a., *On Cyber Warfare*, London: The Royal Institute of International Affairs, 2010 (Chatham House Report), S. 25–34.

32 Zitiert in Christian Wernicke, »Spionage ist kein Krieg. Der ehemalige CIA-Chef Hayden warnt vor Cyber-Attacken, aber auch vor Hysterie«, in: *Süddeutsche Zeitung*, 23.9.2010, S. 7.

33 Vgl. Europäische Kommission, *Kommission verstärkt Europas Abwehrmaßnahmen gegen Cyberangriffe*, IP/10/1239, Brüssel, 30.9.2010.

34 Farwell und Rohozinski lassen durchblicken, dass ihrer Meinung nach Israel und USA für die Angriffe verantwortlich sind. Vgl. James P. Farwell/Rafal Rohozinski, »Stuxnet and the Future of Cyber War«, in: *Survival*, 53 (Februar–März 2011) 1, S. 23–40; David E. Sanger, »Obama Order Sped Up Wave of Cyberattacks against Iran«, in: *New York Times*, 1.6.2012; vgl. ders., *The Inheritance. The World Obama Confronts and the Challenges to American Power*, New York: Random House 2012 (im Erscheinen).

35 Uwe Proll, »Nach A-Waffen die IT-Waffen. Stuxnet verändert die globale Sicherheitsarchitektur«, in: *Behörden Spiegel*, November 2010, S. 1.

36 Vgl. »Computerschädling Flame: Experten enttarnen neue Cyberwaffe«, in: *Spiegel Online*, 28.5.2012; »Cyber-Attacke: Israel preist Spionage-Virus Flame«, in: *Spiegel Online*, 29.5.2012.

37 Frank Rieger, »Stuxnet: Angriff ist besser als Verteidigung«, in: *Frankfurter Allgemeine Zeitung*, 17.1.2011.

38 Zitiert nach Proll, »Nach A-Waffen die IT-Waffen« [wie Fn. 35].

39 Interview mit Sandro Gaycken, »Mit Cyber-Kriegen lassen sich geostrategische Ziele realisieren«, in *Zeit Online*, 8.2.2012.

Die Mehrebenen- und Multistakeholder-Struktur der Cybersicherheitspolitik

Betrachtet man die großen Herausforderungen sowohl für die Wirtschaft als auch für die nationale Sicherheit, drängt sich die Frage auf, wie sich europäische Cybersicherheitspolitik institutionell einbetten ließe. Die Governance heutiger Cybersicherheitspolitik vereint einen ordnungspolitischen Liberalismus, der die Rolle privater Akteure unterstreicht, mit einer klaren Betonung der Rolle des Staates für die nationale Sicherheit. Auffällig ist auch die Pluralität der Akteure. An ihr ist abzulesen, dass die Herausforderung sehr dynamisch ist und dass zwischen den verschiedenen Institutionen nicht eindeutig geklärt ist, wer wofür zuständig und verantwortlich ist. Die Praxis der Cybersicherheitspolitik behilft sich hier mit dem Begriff des Multistakeholder-Ansatzes. Er läuft darauf hinaus, all jenen die Teilhabe zu ermöglichen, die entweder über relevantes Expertenwissen (Unternehmen) oder politische Autorität (Staaten) verfügen. Die Kenntnis wesentlicher Strukturen und Akteure der Cybersicherheitspolitik auf der internationalen, regionalen und nationalen Ebene ist notwendig, um Leitlinien für die Regulierung formulieren zu können, die nicht nur Effektivitäts-, sondern auch hinreichenden Legitimitätskriterien genügen.

Staatliche Ebene

Einerseits ist das globale Internet ein hochgradig entgrenzter Raum, andererseits obliegt seine politische Verregelung und die Beförderung von Sicherheit noch immer dem Nationalstaat. Nur auf staatlicher Ebene lassen sich Straftatbestände kodifizieren, Verfahren der Strafverfolgung etablieren und Sanktionen gegen Regelbrüche durchsetzen.[40] Die staatliche Ebene ist es, auf der wichtige Meinungsbildungsprozesse stattfinden und die sowohl europäische als auch internationale Regelsetzungsprozesse an den demokratischen Diskurs anbindet. Und es ist der Staat, der allein über die Kompetenzen und Möglichkeiten verfügt, nationale Sicherheit zu gewährleisten und die hierfür notwendigen Maßnahmen zu ergreifen. Es ist deshalb auch die nationale Ebene, auf der heikle Fragen besprochen und entschieden werden, etwa wie tief staatliche Sicherheitsmaßnahmen in individuelle Freiheiten eingreifen dürfen.

In allen Staaten der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development, OECD) wurden daher in den letzten Jahren die Anstrengungen verstärkt, staatliche Institutionen und private Unternehmen besser vor Angriffen aus dem Internet zu schützen.[41] Dabei spielen die USA eine führende Rolle. Die US-Administration unter Präsident Obama hat das Thema Cyber Security zu einer Priorität für ihre Verteidigungs- und Heimatschutzpolitik erklärt. In den USA sollen in den nächsten fünf Jahren rund 30 Milliarden Dollar für die Cybersicherheit bereitgestellt werden. Es wird sogar diskutiert, ob der Präsident einen »kill switch« erhalten soll, einen Kippschalter, der es ihm erlaubt, das gesamte Internet in den USA herunterzufahren. In Europa kommt eine solche Vorgehensweise bisher nicht in Frage. Die Netze der relevanten Anbieter (Deutsche Telekom, France Télécom, British Telecom und Telefónica) ziehen sich durch zahlreiche europäische Staaten, so dass rein nationale Maßnahmen so gut wie ausgeschlossen sind.

In den einschlägigen Veröffentlichungen werden China und Russland immer wieder beschuldigt, von ihrem Territorium ausgehende Cyberangriffe auf Regierungsstellen, Unternehmen oder kritische Infrastrukturen entweder zu dulden oder sogar aktiv zu unterstützen.[42] Bundesinnenminister Hans-Peter Friedrich zufolge gibt es klare Anhaltspunkte dafür, »dass vielen Cyber-Angriffen eine IP-Adresse aus dem

40 Einen Vergleich mit nationalen Cybersicherheitsstrategien zieht Alexander Seger, *Cybercrime Strategies*, Straßburg: Council of Europe, 14.10.2011 (Diskussionspapier).

41 Die US-Regierung will zum Beispiel die neue Abwehrtechnik »Einstein 3« einsetzen. Damit möchte sie kritische Infrastrukturen in der Wirtschaft schützen und den Internetverkehr in Echtzeit nach verdächtigen Datenpaketen filtern. Vgl. Ulrich Hottelet, »Digitale Aufrüstung«, in: *Die Zeit*, 2.2.2012, S. 22.

42 Als Beispiele hierfür stehen Richard Clarke, »China's Cyberassault on America«, in: *The Wall Street Journal*, 15.6.2011; Mike McConnell/Michael Chertoff/William Lynn, »China's Cyber Thievery Is National Policy – and Must Be Challenged«, in: *The Wall Street Journal*, 27.1.2012.

Adressraum China zugrunde liegt«.[43] Selbst deutsche Regierungsstellen wurden zur Zielscheibe von Attacken aus China. Auch der US-Militärgeheimdienst NSA (National Security Agency) listet chinesische Rechner als die Orte auf, von denen aus immer wieder Spionageangriffe auf Unternehmen und Regierungsbehörden gestartet werden. Ähnliche Vorwürfe richten sich an Russland. Der islamische Fundamentalismus hingegen scheint bei den Bemühungen um mehr Cybersicherheit interessanterweise allenfalls eine Nebenrolle zu spielen.[44]

Seit einigen Jahren wird auch in Deutschland versucht, der verschärften Bedrohungslage vor allem mit mehr Abwehrmaßnahmen zu begegnen.[45] Die 2010 von der Innenministerkonferenz gebilligte Strategie zur Bekämpfung der Cyberkriminalität empfiehlt unter anderem, den Informationsaustausch zwischen öffentlichen Dienststellen und privaten Akteuren zu verbessern, die Kriminalität wirksamer zu kontrollieren, das Verantwortungsbewusstsein bei Anbietern und Entwicklern zu fördern sowie die Kompetenz privater und professioneller Anwender zu erhöhen. Übungen wie LÜKEX 2011 und die Teilnahme Deutschlands an der US-Übung Cyberstorm 2010 oder an Eurocybex 2010 sind Teil der Sicherheitsmaßnahmen. Auch der Koalitionsvertrag von CDU/CSU und FDP enthält konkrete Vorgaben dafür, wie mehr Cybersicherheit zu schaffen wäre. So soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestärkt und zur zentralen Cybersicherheitsbehörde ausgebaut werden. Weiterhin sollen Kompetenzen innerhalb der Regierung bei der Beauftragten der Bundesregierung für Informationstechnik gebündelt werden. Im Februar 2011 hat die Bundesregierung zudem eine Cybersicherheitsstrategie verabschiedet, deren zentrales institutionelles Element der Aufbau eines Nationalen Cyber-Abwehrzentrums (NCAZ) ist. Beteiligt daran sind unter anderem das BSI, das Bundeskriminalamt, der BND, das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie die Bundespolizei, das Zollkriminalamt und die Bundeswehr. Letztere bringt ihre Erkenntnisse ein, die sie bei der Arbeit des Kommandos strategische Aufklärung und der dort als Einheit zur Kriegführung im Cyberspace angesiedelten »Gruppe Computer Netzwerk Operationen« gesammelt hat.[46] Die Bundeswehr attestiert sich selbst sogar eine »Anfangsbefähigung« für Attacken in »gegnerischen Netzen«.[47]

Inwiefern das Cyberabwehrzentrum imstande sein wird, dauerhaft für mehr Sicherheit von Regierungsinstitutionen, kritischen Infrastrukturen und privaten Unternehmen zu sorgen, wird im Wesentlichen davon abhängen, wie effektiv es Expertenwissen und Ressourcen der beteiligten Institutionen zusammenführen kann. Die Verdichtung von Wissen, die Verknüpfung von Ressourcen und die Kommunikation mit anderen europäischen und internationalen Gremien müssen im Mittelpunkt seiner Arbeit stehen. Die magere Ausstattung mit lediglich zehn Beamten lässt jedenfalls nicht erwarten, dass das NCAZ eigenständig in der Lage sein wird, Bedrohungen zu identifizieren und angemessene Gegenmaßnahmen zu entwickeln.

An den Strukturen der deutschen Cybersicherheitspolitik lässt sich gut ablesen, wie die ehemals scharfen Grenzen zwischen innerer und äußerer Sicherheit und zwischen den verschiedenen Ressorts verschwimmen. Die traditionelle Aufgabenteilung zwischen Zivilschutz, militärischer Verteidigung und Polizei gerät ebenso ins Wanken wie die überkommene Vorstellung, öffentliche Gewalt und privates Unternehmertum seien streng voneinander geschieden. Dass die Grenze zwischen öffentlicher Gewalt und privaten Akteuren mehr und mehr verwischt wird, zeigen besonders die Bemühungen um den Aufbau sogenannter Computer Emergency Response Teams (CERTs).[48]

43 Vgl. »Bundesinnenminister Friedrich zur Cybersicherheit: ›Es ist richtig, die Alarmglocken zu läuten‹«, in: *Stern*, 15.3.2012.

44 Siehe zur Problematik Cyberjihadismus Asiem El Difraoui, *jihad.de. Jihadistische Online-Propaganda: Empfehlungen für Gegenmaßnahmen in Deutschland*, Berlin: Stiftung Wissenschaft und Politik, Februar 2012 (SWP-Studie 5/2012), S. 22f.

45 Zu den Ausführungen bundesdeutscher Politik vgl. Klaus-Dieter Fritsche, *Cyber-Sicherheit. Die Sicherheitsstrategie der Bundesregierung*, Sankt Augustin: Konrad-Adenauer-Stiftung, März 2011 (Analysen und Argumente; 89).

46 Ergänzt wird das technisch-operative Zentrum durch einen Nationalen Cyber-Sicherheitsrat. Neben Vertretern des Bundeskanzleramts gehören ihm zahlreiche Staatssekretäre an, nämlich des Auswärtigen Amtes, des Bundesinnenministeriums, des Bundesverteidigungsministeriums, des Bundeswirtschaftsministeriums, des Bundesjustizministeriums, des Bundesfinanzministeriums sowie der Länder. Je nach Anlass sollen auch Wirtschaftsvertreter assoziiert werden.

47 Siehe hierzu »Bundeswehr bereit für Cyberangriffe«, in: *Zeit Online*, 5.6.2012.

48 Zu Multistakeholder-Sicherheit, auch im Kontext von CERTs, siehe Andreas Schmidt, »At the Boundaries of Peer Production: The Organization of Internet Security Production in the Cases of Estonia 2007 and Conficker«, in: *Telecommunications Policy*, 36 (Juli 2012) 6, S. 451–461; Michel J. G. Van Eeten u.a., »The Governance of Cybersecurity: a Framework for Policy«, in: *International Journal of Critical Infrastructures* 2 (2006) 4, S. 357–378.

Diese sammeln Informationen über Computerangriffe, entwerfen Pläne für den Umgang mit ihnen und etablieren nationale Abwehrmaßnahmen. In den meisten Fällen koordinieren sie dabei privates und öffentliches Expertenwissen, um auch diejenigen Unternehmen einzubinden, die von Angriffen betroffen sind. Gerade bei Firmen, die im Besitz »kritischer Infrastrukturen« sind (Energie, Verkehr, Gesundheit und anderes), handelt es sich um Schutzaufgaben, die weit über die Interessen der jeweiligen Aktionäre hinausgehen, denn die ungestörte Funktionsweise der genannten Strukturen liegt im Interesse der gesamten Gesellschaft und damit auch des Staates.

Internationale Ebene

Effektive Rechtssetzungen bei der Cybersicherheit lassen sich kaum mehr auf den Nationalstaat begrenzen. Zwar bleibt er für die nationale Sicherheit und den Schutz von Privateigentum außerordentlich wichtig. In einer entgrenzten Struktur kann er aber allein kaum noch wirksam handeln. Deshalb müssen nationale Bestimmungen international miteinander harmonisiert werden. Straftaten können im Cyberspace aus einem Staat heraus verübt werden, in dem es keine einschlägigen strafrechtlichen Bestimmungen gibt und die rechtliche Grundlage für jede Form der Strafverfolgung fehlt (Problematik des »sicheren Hafens«). In vielen Staaten ist beispielsweise das Einbrechen in fremde Datenbanken nur dann strafbar, wenn auch eine direkte Schädigung eines anderen nachgewiesen werden kann. Wen also sollten die deutschen Strafverfolgungsbehörden mit Hilfe welcher Instrumente belangen, wenn Angriffe auf staatliche Infrastrukturen von einem Ort aus verübt werden, an dem dies nicht als Straftatbestand betrachtet wird?

Im Folgenden wird ein Überblick über bedeutende formelle und informelle gouvernementale und nichtstaatliche Akteure auf der internationalen Ebene gegeben. Er zeigt, wie breit die Palette von Institutionen und Akteuren mit ihren jeweiligen Interessen ist und welche Strategien sie anwenden, um Gefahren für Privateigentum und staatliche Sicherheit abzuwenden. Wichtige Impulse für die Cybersicherheit gingen von der Generalversammlung der Vereinten Nationen (VN) aus, aber auch von anderen Organisationen, insbesondere der International Telecommunication Union (ITU), der Gruppe der 20 wichtigsten Industrie- und Schwellenländer (G20), der Gruppe der acht größten Industrienationen (G8), der Nato, der Shanghai-Gruppe und von Interpol. Ebenfalls auf diesem Feld tätig ist eine Reihe transnationaler Foren, regionaler Organisationen und nichtstaatlicher Organisationen.

Internationale Organisationen

Die VN-Generalversammlung befasst sich ausgiebig mit der Cybersicherheit, was sich in zahlreichen Resolutionen niederschlug. Im Sozial- und Wirtschaftsausschuss der VN wurden die Resolutionen 56/121 (»Combating the Criminal Misuse of Information Technology«, 2002) und 57/239 (»Creation of a Global Culture of Cybersecurity«, 2003) angenommen. Beide richten sich gegen Staaten, die den Cyberraum gar nicht oder nur mangelhaft regulieren, und gegen die Gefahr, dass von dort aus Angriffe auf Unternehmen oder Staaten lanciert werden. Im Bericht 64/422 (»Globalization and Interdependence«, 2009) werden VN-Mitgliedstaaten aufgefordert, ihre Kapazitäten zur Abwehr von Angriffen auf kritische Infrastrukturen zu überprüfen. Im Abrüstungsausschuss wurde Resolution 64/386 (»Developments in the Field of Information and Telecommunication in the Context of International Security«, 2009) verabschiedet. Die daraufhin eingesetzte VN-Kommission warnte unter anderem davor, dass Staaten immer mehr Cyberwarfare-Kapazitäten aufbauen.[49] Der VN-Bericht über Cybersicherheit von 2010 stieß eine breite Debatte darüber an, ob und inwieweit die etablierten völkerrechtlichen Prinzipien und Normen auch im Cyberspace gelten.[50] Auf der operativen Ebene der VN ist die ITU in den letzten Jahren zu einem wesentlichen Akteur geworden.[51] Sie organisiert das Internet Governance Forum (IGF), die World Conference on International Telecommunications (WCIT) und den World Summit on the Information Society (WSIS).[52] Die WCIT ist eine rein intergouvernementale Konferenz und überarbeitet die International Telecommunications Regulations (ITR), einen völkerrechtlichen Vertrag aus dem Jahr 1988.

49 UN 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/65/201, 30.7.2010.

50 Jeffrey Carr, *Inside Cyber Warfare. Mapping the Cyber Underworld*, Sebastopol, CA, 2010, Kapitel 3.

51 ITU, <http://www.itu.int> (eingesehen am 20.3.2012).

52 ITU, *World Conference on International Telecommunications (WCIT-12)*, <http://www.itu.int/en/wcit-12/Pages/default.aspx> (eingesehen am 20.3.2012). Einen Überblick zum WSIS-Prozess bietet Milton L. Mueller, *Networks and States. The Global Politics of Internet Governance*, Cambridge, MA: MIT Press, 2010.

Gleichwohl ist diese Überarbeitung alles andere als unumstritten. Sie ist symptomatisch für einen tiefgreifenden Konflikt innerhalb der Staatenwelt über die angemessene Regelungsphilosophie in allen Fragen, die das Spannungsfeld zwischen staatlicher Sicherheit und privater Freiheit betreffen. Auf der einen Seite finden sich etliche Staaten, die rechtlich verbindliche Vorschriften für nahezu alle Aspekte im Zusammenhang mit dem Internet in den Vertrag einbauen wollen. Die Shanghai-Gruppe (Russland, China, Usbekistan und Tadschikistan) hat 2011 hierzu vorgeschlagen, einen zwischenstaatlichen Internet-Verhaltenskodex auszuarbeiten. Dieser soll »Normen und Regeln für das Verhalten von Staaten im Cyberspace« festlegen. In einer VN-Resolution vom Dezember 2011 wird der VN-Generalsekretär aufgefordert, »weiterhin bestehende und potenzielle Bedrohungen auf dem Gebiet der Informationssicherheit und mögliche kooperative Maßnahmen zu deren Bewältigung, einschließlich Normen, Regeln oder Prinzipien eines vertrauensbewussten Handelns der Staaten und vertrauensbildende Maßnahmen im Hinblick auf den Informationsraum«[53] zu identifizieren. Dahinter steht die Idee, dass die von Aktivitäten im Internet bedrohte Souveränität von Staaten gestärkt und dass jede Einmischung in die inneren Angelegenheiten eines Staates, die über das Internet erfolgt, verboten werden müsse.

Der von den VN aufgenommene Vorstoß der Shanghai-Gruppe stößt allerdings gerade bei den USA auf wenig Gegenliebe. Er repräsentiert eine ordnungspolitische Vorstellung, die quer zum dezentralen Multistakeholder-Ansatz der USA liegt. Internationale Verträge in der Cyberpolitik gelten den Vereinigten Staaten als zu starr, zu wenig verifizierbar und zu sehr auf staatliches Handeln fokussiert, um asymmetrischen Cyberbedrohungen entgegenwirken zu können. Zudem dürften die USA sich ihrer technologischen Vormachtstellung in allen Fragen des Internets bewusst sein und daher wenig Interesse an einer globalen Regulierung haben. Stattdessen setzen sie auf einen intensivierten internationalen Dialog über Verhaltensnormen und vertrauensbildende Maßnahmen sowie die Einbindung nichtstaatlicher Akteure, wie sich der im Mai 2011 von US-Präsident Obama verkündeten International Strategy for Cyberspace entnehmen lässt.

Mehr Unterstützung seitens der USA findet die 2010 gegründete Improvement Working Group, die das IGF weiterentwickeln will. Dieses baut auf dem Multistakeholder-Ansatz auf und bringt Regierungen, Privatwirtschaft, technische Experten und Zivilgesellschaft zusammen. Doch auch hier sind die Meinungsbildungsprozesse eher mühsam. Während einige Staaten verbindliche Beschlüsse fassen wollen, loben andere die formelle Unverbindlichkeit einer freien Diskussion jenseits von Stakeholder-Grenzen. Strittig ist auch die zukünftige Rolle des IGF im Kontext anderer Institutionen. Vor allem China und Russland versuchen zu vermeiden, dass der IGF erstarkt und nichtstaatliche Akteure auf diese Weise ihren Einfluss vergrößern. Wie unterschiedlich die USA und Russland an die Frage der angemessenen Organisation globaler Cybersicherheitspolitik herangehen, zeigt sich auch in der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE).[54] Die russische Seite verfolgt die Idee einer universellen Cyberkonvention, die Normen angemessenen staatlichen Verhaltens kodifizieren soll. Die USA lehnen diesen Plan ab und betonen, nationalstaatliche Regelungen hätten Vorrang.[55] Deutschland bezieht in dieser Frage derzeit eine vermittelnde Position. Auf der Computermesse CeBIT 2011 hatte die Bundeskanzlerin dafür geworben, für staatliches Verhalten im Cyberraum einen Kodex zu formulieren, der von möglichst vielen Staaten unterzeichnet werden solle. Unklar ist noch, welche der internationalen Organisationen (G8, G20, Europarat, EU, Nato, OSZE, VN) hierfür der richtige Ansprechpartner ist. Die deutsche Bundesregierung sieht die Europäische Agentur für Netzwerk- und Informationssicherheit (European Network and Information Security Agency, ENISA) zumindest auf der operativen Ebene in der Pflicht.

Inzwischen ist auch Interpol in die Regulierung des Internets eingebunden.[56] Die Organisation plant, 2014

53 UN General Assembly, *General Assembly, Gravely Concerned about Status of UN Disarmament Machinery, Especially in Conference on Disarmament, Invites States to Explore Options*, GA/11182, New York, 2.12.2011 (Zitat bei Kleinwächter, »Kalter Krieg im Cyberspace« [wie Fn. 9]).

54 Siehe hierzu United States Mission to the OSCE, *Cyber Security Keynote Address by Dr. Deborah Schneider, U.S. Department of State*, FSC-PC.DEL/30/10, 9.6.2010, <http://www.osce.org/fsc/68524> (eingesehen am 23.2.2012).

55 Vgl. Franz-Stefan Gady/Greg Austin, *Russia, the United States, and Cyber Diplomacy. Opening the Doors*, New York: EastWest Institute, 2010; *Statement by Mr. S. Shestakov, Representative of the Russian Federation, at the Joint Meeting of the OSCE Forum for Security Co-operation and the OSCE Permanent Council*, FSC-PC.DEL/31/10, 10.6.2010, <www.osce.org/fsc/68693> (eingesehen am 23.3.2012).

56 Eine Übersicht über die rechtlichen Grundlagen von

in Singapur eine zentrale Forschungs- und Ermittlungsstelle zur Bekämpfung von Cybercrime einzurichten (Interpol Global Complex for Innovation, IGCI).[57] Das Institut wird über Forschungs- und Entwicklungsmöglichkeiten, Schulungseinrichtungen und moderne computerforensische Labors verfügen. Ein weiterer Schwerpunkt soll auf der Evaluierung und Weiterentwicklung von Open Source Software für die Strafverfolgungsbehörden liegen. Zudem sollen Länder unterstützt werden, die selbst über keine ausreichenden Ressourcen zur Bekämpfung von Cybercrime verfügen.

Die G8-Staaten konnten sich ebenfalls weitgehend reibungslos auf Maßnahmen verständigen. So soll eine gemeinsame Arbeitsgruppe zur Bekämpfung der Hightechkriminalität gegründet werden, die sogenannte Lyon-Rom-Gruppe. Ferner soll ein rund um die Uhr erreichbares Informationsnetz aufgebaut werden. Es soll rasche Kontaktaufnahme in all jenen Fällen gestatten, in denen elektronisches Beweismaterial vorliegt und dringend Amtshilfe ausländischer Strafverfolgungsbehörden benötigt wird.

Regionale internationale Organisationen

Wie stark globale ordnungspolitische Differenzen wirken können, wird besonders deutlich, wenn man die Einigungsfähigkeit globaler internationaler Organisationen betrachtet. In regional spezifischeren internationalen Organisationen finden sich regulatorische Dynamiken, die weit über das hinausgehen, was im Kontext der VN erreicht wurde. Das wohl wichtigste regionale Abkommen auf dem Gebiet der Cybersicherheit ist das Europarats-Übereinkommen über Cyberkriminalität aus dem Jahr 2001 (seit 2004 in Kraft). Es enthält gemeinsame Definitionen der verschiedenen Arten von Internetkriminalität und bildet die Grundlage für eine engere justizielle Zusammenarbeit zwischen den Mitgliedstaaten des Europarats sowie einigen außereuropäischen Staaten, insbesondere den USA und Kanada. Überdies haben zahlreiche Länder (darunter die USA und alle EU-Staaten) ein Zusatzprotokoll über die strafrechtliche Verfolgung rassistischer oder fremdenfeindlicher Handlungen ratifiziert.[58] Weiterhin haben sowohl der Europarat als auch die OECD Grundsätze für ein sicheres Internet erarbeitet.[59] Beide Organisationen unterstreichen Universalität und Integrität eines sicheren und stabilen Internets. Dort heißt es auch, dass private Akteure in die Formulierung neuer Regeln eingebunden werden sollen. Schließlich soll die bestehende Architektur des Internets mit seinen offenen Standards und der dezentralen Verwaltung beibehalten werden. Im Europarat wird ebenfalls intensiv darüber nachgedacht, private Akteure am intergouvernementalen Verhandlungsprozesses zu beteiligen.

Auch die Nato hat in den letzten Jahren bemerkenswerte Fortschritte auf dem Weg zu einer effektiven Cybersicherheitspolitik gemacht.[60] In ihrem neuen Strategischen Konzept hat sie sich nicht nur zum Ziel gesetzt, ihre eigenen Fähigkeiten zur Abwehr militärischer Cyberangriffe zu verbessern. Darüber hinaus bietet sie den Mitgliedstaaten auf freiwilliger Basis Sicherheitsstandards für kritische Infrastrukturen an.[61] Die im Juni 2011 beschlossene Nato Cyber Defence Policy hebt die Relevanz der Cybersicherheit hervor und institutionalisiert eine formale Struktur für die politische Koordination. Die neu gegründete Nato Cyber Defence Management Authority (CDMA) hat die Verantwortung für Koordination und strategische Entscheidungen im Bereich der Cyberdefence erhalten. Die ebenfalls neu gegründete Emerging Security Challenges Division koordiniert die politische und strategische Übersicht über die Abwehrmaßnahmen der Nato. Das Computer Incident Response Capability – Technical Centre (NCIRC TC) ist für operative Maßnahmen zuständig, das Cooperative Cyber De-

Cyberkriminalitätsbekämpfung verschiedenster Akteure bietet Marco Gercke, *Understanding Cybercrime: a Guide for Developing Countries*, 2. Aufl., Genf: ITU, März 2011; siehe auch die etwas ältere Studie der ITU Global Cybersecurity Agenda (GCA) – High Level Experts Group (HLEG), *Global Strategic Report*, Genf: ITU, 2008.

57 Interpol, *The INTERPOL Global Complex for Innovation*, <http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation> (eingesehen am 23.2.2012).

58 Council of Europe, *Cybercrime*, <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp> (eingesehen am 20.3.2012).

59 Vgl. OECD, *Communiqué on Principles for Internet Policy Making*, <www.oecd.org/dataoecd/40/21/48289796.pdf>, sowie Council of Europe, *Internet Governance Principles*, <www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf> (eingesehen am 21.1.2012).

60 Nato, *NATO and Cyber Defence*, <http://www.nato.int/cps/en/SID-E1098959-0D8780E1/natolive/topics_78170.htm?> (eingesehen am 20.3.2012).

61 Vgl. Nato, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, 19.11.2010, <http://www.nato.int/cps/en/natolive/official_texts_68580.htm> (eingesehen am 20.3.2012).

fence Centre of Excellence (CCD COE) schließlich fungiert als Schnittstelle zwischen Bündnis, Wissenschaft und Öffentlichkeit.

Die Maßnahmen des Europarats und der Nato bauen auf einer langjährigen und engen Zusammenarbeit ihrer Mitgliedstaaten auf. Nur auf dieser Basis lässt sich eine rechtlich verbindliche internationale Regulierung des Internets erreichen. Notwendig sind ein Mindestmaß an zwischenstaatlichem Vertrauen und weitgehend deckungsgleiche Vorstellungen über das angemessene Verhältnis zwischen individueller Freiheit, liberaler Marktwirtschaft und öffentlicher Autorität. In Europa sowie zwischen Europa und den USA sind diese Bedingungen im Großen und Ganzen erfüllt. Zwischen dem transatlantischen Raum einerseits und den Staaten jenseits davon andererseits herrschen dagegen oftmals Misstrauen und wechselseitige Vorwürfe, insbesondere in den Beziehungen zu China und Russland. Daher dürfte kaum zu erwarten sein, dass die Staatengemeinschaft mittelfristig eine globale Regulierung des Internet verwirklichen kann, die diesen Namen verdient, und daher auch keine umfassende Abwehr von Bedrohungslagen gewährleisten kann. Zu befürchten ist vielmehr, dass zwei Cyberwelten mit unterschiedlichen regulatorischen Standards entstehen. Dies dürfte Freiheit und Sicherheit im Internet nicht unwesentlich beeinträchtigen.

Transnationale Foren

Die Strategie der USA und anderer westlicher Staaten zur Gestaltung von Cybersicherheitspolitik baut überwiegend auf den positiven Erfahrungen auf, die in den letzten Jahren mit einigen transnationalen Foren, also einer stärkeren Einbeziehung privater Akteure, gemacht worden sind.[62] Ein Beispiel hierfür ist das Forum of Incident Response and Security Teams (FIRST). Auf FIRST-Konferenzen tauschen gouvernementale und nichtgouvernementale IT-Sicherheitsexperten Informationen und Erfahrungen im Umgang mit Angriffen und Malware aus und bauen persönliche Vertrauensbeziehungen auf. FIRST akkreditiert zudem nationale und nichtstaatliche CERTs und unterbreitet Vorschläge für deren Verbesserung. Aktuell versuchen FIRST und ITU ihre jeweiligen Aktivitäten zu koordinieren, damit öffentliches und privates Expertenwissen sich sinnvoll ergänzen. Im Idealfall soll sich eine neue Form der öffentlich-privaten Partnerschaft herausbilden, die politische Autorität und privates Wissen kombiniert und neue transnationale Lösungen erlaubt.

Neben seinen nationalstaatlichen, internationalen, regionalen und transnationalen Säulen enthält der von den USA und anderen westlichen Staaten bevorzugte Multistakeholder-Ansatz auch die Idee, dass private Akteure eigenständig ihr Expertenwissen organisieren. Beispiele auf der internationalen Ebene sind die Internet Engineering Task Force (IETF), das Institute of Electrical and Electronics Engineers (IEEE), die Internet Corporation for Assigned Names and Numbers (ICANN), die International Cyber Security Protection Alliance (ICSPA) und das Financial Services – Information Sharing and Analysis Center (FS-ISAC). Alle diese privatwirtschaftlich betriebenen Organisationen verfolgen den Zweck, entweder selbst Abwehrmaßnahmen gegen Cyberangriffe zu koordinieren und geeignete Instrumente für die private Wirtschaft zu entwickeln oder aber staatliche und zwischenstaatliche Institutionen mit ihren Kenntnissen zu unterstützen. Darin offenbart sich die in den USA und Europa gängige Einsicht, dass staatliche Institutionen in vielen Fällen damit überfordert sind, die wichtigsten Herausforderungen selbst zu identifizieren und angemessene Antworten zu finden. Diese Einsicht ist eine Grundlage des ordnungspolitischen Liberalismus des Westens, was die Regulierung des Internets betrifft. In ihr dokumentiert sich auch der wesentliche Unterschied zum regulatorischen Ansatz Russlands und Chinas.

Älteste nichtstaatliche Plattform im Bereich der technischen Entwicklung des Internets ist die IETF.[63] Sie besteht seit 1986 und versammelt viele der Softwareprogrammierer, die das Internet maßgeblich vorangebracht haben. Die Organisation kennt weder eine strikt hierarchische Struktur noch eine klar definierte Mitgliedschaft: »We reject kings, presidents and voting. We believe in rough consensus and running codes.«[64] Anhand dieser Methode werden seit Ende der 60er Jahre die RFCs (Request for Comments) für das sogenannte Internet Law Book geschrieben. So folgen die Politiken der Regional Internet Registries (RiRs), die die IP-Adressen zuordnen, keinem von

62 Siehe hierzu grundlegend *PPPs in der Sicherheitspolitik: Chancen und Grenzen*, Zürich: CSS, April 2012 (CSS Analysen zur Sicherheitspolitik; 111).

63 The Internet Engineering Task Force (IETF), <http://www.ietf.org> (eingesehen am 22.3.2012).

64 *The Tao of IETF*, Punkt 3, <http://www.ietf.org/tao.html#anchor3> (eingesehen am 22.3.2012).

Regierungen unterzeichneten völkerrechtlichen Vertrag, sondern werden auf der Basis von RFCs ausgehandelt, die von der IETF genehmigt werden.[65] Eine ebenfalls private, nicht gewinnorientierte Institution ist das IEEE, das inzwischen mehr als 350 000 Mitglieder hat. Es beschäftigt sich vorwiegend mit Fragen der Konnektivität zwischen unterschiedlichen Geräten (also den Möglichkeiten, diese untereinander zu verbinden) und der Harmonisierung technischer Standards.

Was Normenentwicklung und Zuweisung von IP-Adressen anbelangt, ist die ICANN besonders hervorzuheben. Es handelt sich um eine nicht gewinnorientierte gemeinnützige Organisation, die nach den Gesetzen des Staates Kalifornien operiert und ihren Sitz an der University of South California hat.[66] Vertraglich ist die ICANN eine quasi-autonome Nichtregierungsorganisation (Quasi-autonomous Non-governmental Organization, QANGO) und arbeitet eng mit dem US Department of Commerce zusammen.[67] Die US-Regierung übt weitaus mehr Einfluss auf die ICANN aus als andere darin vertretene Regierungen, was viele Staaten sehr kritisch sehen. Im Oktober 2011 haben Indien, Brasilien und Südafrika (die sogenannten IBSA-Staaten) vorgeschlagen, einen neuen zwischenstaatlichen VN-Ausschuss für Internetpolitik (Committee for Internet-Related Policies, CIRP) einzurichten. Dieser solle nicht nur die ICANN, sondern auch andere technische Internetorganisationen beaufsichtigen. Demnach soll er auch eine Art Gerichtshof werden, der von Regierungen kontrolliert wird.

Eine weitere nicht gewinnorientierte Vereinigung privater Unternehmen ist die 2011 gegründete ICSPA.[68] Sie ist nicht zuletzt deswegen interessant, weil sie staatliche Strafverfolgungsbehörden mit Expertenwissen und sogar mit materiellen Ressourcen unterstützt und damit direkt in Kernbereiche staatlicher Souveränität vordringt.[69] Zu den Gründungsmitgliedern zählen neben IT-Security-Spezialisten wie Trend Micro und McAfee der Finanzdienstleister Visa Europe und die große britische Online-Handelsgruppe Shop Direct. Die Organisation kooperiert intensiv mit dem Europäischen Polizeiamt (Europol).

In den letzten Jahren wurde zudem eine Reihe sektorspezifischer Cybersicherheitskooperationen aufgebaut. Das FS-ISAC etwa wurde Ende der neunziger Jahre als Reaktion auf die Aufforderung des US-Präsidenten gegründet, dass private und öffentliche Stellen wichtige Informationen zum Schutz gegen Angriffe auf kritische Infrastrukturen austauschen sollen.[70] Das FS-ISAC bündelt Informationen aus der Finanzindustrie, Sicherheitsunternehmen, staatlichen Stellen auf föderaler und einzelstaatlicher Ebene, Strafverfolgungsbehörden und anderen staatlichen und nichtstaatlichen interessierten Parteien, um einen effektiven Schutz gegen Cyberangriffe zu etablieren.

Die Betrachtung der Governance einer entstehenden Cybersicherheitspolitik hat gezeigt, dass demokratische Standards in der globalen Politik wenn überhaupt nur mittelbar eine Rolle spielen, nämlich über das Delegationsprinzip. Parlamente haben ihren Platz in der Cybersicherheitspolitik noch nicht gefunden. Selbst in der Europäischen Union als supranationale Organisation tritt immer offener zutage, wie Prozesse der Entgrenzung von Innen- und Außenpolitik, der Versicherheitlichung von Innenpolitiken und der Privatisierung von Sicherheit das System der Gewaltenteilung in Frage stellen und damit den Kern der Funktionsweise von Demokratien antasten.

65 Vgl. Kleinwächter, »Wie reguliert man den Cyberspace?« [wie Fn. 8].

66 Internet Corporation for Assigned Names and Numbers (ICANN), *Bylaws for Internet Corporation for Assigned Names and Numbers. A California Nonprofit Public-Benefit Corporation*, <www.icann.org/en/general/bylaws.htm> (eingesehen am 15.1.2012).

67 Siehe ICANN, <http://www.icann.org> (eingesehen am 15.1.2012).

68 Siehe ICSPA, <https://www.icspa.org> (eingesehen am 15.1.2012).

69 »Cybercrime-Allianz ICSPA sagt Web-Kriminellen den Kampf an«, in: *TecChannel*, 6.7.2011, <http://www.tecchannel.de/sicherheit/news/2036365/cybercrime_allianz_sagt_web_gangstern_den_kampf_an> (eingesehen am 15.1.2012).

70 Weitere Details sind auf der Webseite von FS-ISAC nachzulesen, <http://www.fsisac.com> (eingesehen am 15.1.2012).

Cybersicherheitspolitik in der Europäischen Union

Die entstehende globale institutionelle Ordnung der Internetregulierung ist auch ein wichtiges Gefüge für die europäische Regulierung. Die EU und ihre Mitgliedstaaten sind in fast alle der genannten Institutionen eingebunden und kooperieren über diese miteinander sowie mit anderen Staaten. Die EU ist allerdings nicht nur ein Akteur innerhalb einer globalen Ordnungsstruktur, sondern gleichzeitig eine eigenständige Ordnungsstruktur für ihre Mitgliedstaaten. Sie ist ein institutionell hochgradig verdichteter grenzüberschreitender Regelungskontext, dessen interne Dynamiken Aufschluss über mögliche Perspektiven globaler Regulierung geben. Das, was wir heute in der EU beobachten, könnte morgen schon auf globale Institutionen und Politik übertragen werden. Präziser gefasst: Die Dynamiken in der EU sind dieselben wie in der internationalen Cybersicherheitspolitik.[71]

Cybersicherheit firmiert inzwischen weit oben auf der politischen Agenda der EU.[72] Die Kommissarinnen Cecilia Malmström und Neelie Kroes sowie die Hohe Vertreterin Catherine Ashton arbeiten derzeit an einer EU-Strategie zur Cybersicherheit. Auf einem transatlantischen Forum in Washington Anfang Mai 2012 umriss Malmström vier Schwerpunkte der Strategie, die nach wie vor als »work in progress« zu verstehen sei. Es gehe um das Verhältnis von Sicherheit und Freiheit in der Prävention, Widerstandsfähigkeit (resilience) und Reaktionsfähigkeiten, öffentlich-private Partnerschaften sowie globale Zusammenarbeit mit Partnern.[73]

Bereits im März 2010 schlug die EU-Kommission einen Aktionsplan vor, mit dem eine konzertierte Strategie zur Bekämpfung der Cyberkriminalität umgesetzt werden könnte.[74] Die Kommission wies darauf hin, dass Cyberrisiken »ihrem Wesen nach grenzüberschreitend« seien und ihre Bekämpfung »angemessene grenzüberschreitende Vorkehrungen« erfordere. Diese sollten unter Einschluss der internationalen Zusammenarbeit mit Drittstaaten[75] getroffen werden, und zwar in Form von Amtshilfe bei der Strafverfolgung. Der EU-Kommission zufolge ist es »nach wie vor wichtig, einen innerhalb der EU kohärenten und auf Zusammenarbeit beruhenden Ansatz zu verfolgen, dieser muss jedoch in eine Strategie der globalen Koordinierung eingebettet sein, in die wichtige Partner (einzelne Länder oder einschlägige internationale Organisationen) einbezogen werden.«[76] Die EU und ihre Institutionen unterhalten daher zu fast allen internationalen Organisationen Kontakte und binden sie in europäische Regelsetzungsprozesse ein, soweit es möglich und zweckmäßig ist. Hier wird ein regulativer Ansatz

71 Ein Beispiel hierfür ist der jüngste Kommissionsvorschlag einer Strategie zum Schutz von Kindern im Netz. Hamadoun Touré, Generalsekretär der ITU, griff diese Idee auf und plädierte für einen weltweiten Code zum Schutz von Kindern im Netz als ein kleiner Schritt auf dem Weg zu einem »Internationalen Code of Conduct für Informationssicherheit«. »New Strategy to Make Internet Safer for Children«, in: *Bulletin Quotidien Europe*, No. 10606, 3.5.2012, S. 7; Monika Ermert, »ITU will globales Abkommen für Cybersecurity vorantreiben«, *Heise Online*, 17.5.2012.

72 Die Trio-Präsidentschaft (Spanien, Belgien, Ungarn) hatte sich mit dem M.A.D.R.I.D.-Report bereits im Mai 2010 explizit dem Thema Cybersicherheit gewidmet. Council of the European Union, *First Main Assessment and Description Report for Internal Debate* (M.A.D.R.I.D. Report), Brüssel, 26.5.2010, <http://register.consilium.europa.eu/pdf/en/10/st10/st10203.en10.pdf>, (eingesehen am 20.1.2012). Nachdem das Papier veröffentlicht war, kündigte EU-Terrorismuskoordinator Gilles de Kerchové an, ein »umfassenderes Konzept für das Vorgehen gegen Cyber-Terrorismus, Cyber-Kriminalität, Cyber-Angriffe und Cyber-Kriege« zu entwickeln. Council of the European Union, *Note from EU Counter-Terrorism Coordinator to Council/ European Council, Subject: EU Counter-Terrorism Strategy*, Discussion Paper, 9685/10, Brüssel, 10.5.2010.

73 Cecilia Malmström, *The European Response to the Rising Cyber Threat*, Transatlantic Cyber Conference Organised by the Center for Strategic and International Studies, the European Security Roundtable and SRA International, Speech/12/315, Washington, D.C., 2.5.2012.

74 Rat der Europäischen Union, *Entwurf von Schlussfolgerungen des Rates zu einem Aktionsplan für die Umsetzung der konzertierten Strategie zur Bekämpfung der Cyberkriminalität*, Brüssel, 25.3.2010, <http://register.consilium.europa.eu/pdf/de/10/st05/st05957-re02.de10.pdf> (eingesehen am 15.1.2012).

75 Auf dem Transatlantischen Rat in Washington im Dezember 2010 wurde beispielsweise das TransAtlantic IPR Portal ins Netz gestellt. Es hat zum Ziel, »to encourage small business (SMEs) to break into foreign markets and avoid risks in terms of the violation of their intellectual property rights (IPR)«. Siehe <http://ec.europa.eu/enterprise/initiatives/ipr/index_en.htm> (eingesehen am 25.3.2012).

76 Europäische Kommission, *Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen* [wie Fn. 14].

angewandt, der den Multistakeholder-Ansatz regional verdichtet und gleichzeitig an die internationale Umgebung ankoppelt.

Eindrückliche Beispiele für diese Ankopplung sind Übungen zur Abwehr von Cyberangriffen. Mittlerweile finden zwischen EU-Staaten und den USA regelmäßig solche Übungen statt. Schon 2010 haben Frankreich, Deutschland, Ungarn, Italien, Niederlande, Schweden und Großbritannien an einer vom US-Ministerium für Innere Sicherheit geleiteten zivil-militärischen US-Übung (Cyber Storm) teilgenommen. Ebenfalls beteiligt waren Australien, Kanada, Japan und Neuseeland sowie 60 private Unternehmen. Im November 2010 wurde die sogenannte High-Level EU-US Working Group on Cybersecurity and Cybercrime[77] eingerichtet, die »ein gemeinsames Programm und ein(en) Fahrplan für gemeinsame transkontinentale Übungen zur Internetsicherheit« erarbeiten soll.[78] Bei der Übung Cyber Atlantic 2011 schließlich simulierten Experten aus mehr als 20 Ländern Angriffe, zum Beispiel auf Kraftwerke, um die Zusammenarbeit zwischen den Ländern zu testen.

Die Verschmelzung von Innen- und Außenpolitik

Eine auffällige Entwicklung ist die Verschmelzung europäischer Innen- und Außenpolitik. Wenn es in einem globalen Raum kein Innen und Außen mehr gibt, lässt sich auch die Trennung zwischen Innen- und Außenpolitik nicht sinnvoll aufrechterhalten. Die wichtigsten Anstöße zur Formulierung einer europäischen Cybersicherheitspolitik in den letzten Jahren kamen aus einer engen Kooperation zwischen Institutionen aus Innen- und Justizpolitik einerseits sowie Außen- und Sicherheitspolitik andererseits. Institutionell findet diese Zusammenarbeit ihren Niederschlag in gemeinsamen Sitzungen des Politischen und Sicherheitspolitischen Komitees (PSK) und des Ständigen Ausschusses des Rats für die operative Zusammenarbeit bei der inneren Sicherheit (Standing Committee on Operational Cooperation on Internal Security, COSI) sowie den Parlamentsausschüssen für bürgerliche Freiheiten, Justiz und Inneres (Committee on Civil Liberties, Justice and Home Affairs, LIBE) und für auswärtige Angelegenheiten (Committee on Foreign Affairs, AFET).[79]

In diesen Sitzungen hat sich herausgestellt, dass die Bereiche innere Sicherheit und Außenpolitik sich nur noch schwer auseinanderhalten lassen. Kritische Infrastrukturen, etwa bei Energie, Gesundheit, Verkehr oder Kommunikation, lassen sich heute nicht mehr vor Attacken bewahren, wenn nur außenpolitische oder nur innenpolitische Maßnahmen ergriffen werden. In einer Mitteilung vom 31. März 2011 zum Schutz kritischer Informationsinfrastrukturen[80] warnt die Kommission vor den Gefahren von Cyberterrorismus und Cyberkrieg und verlangt bessere interne Abwehrmaßnahmen gegen Bedrohungen von außen. Im Ratsdokument 10299/11 wird eine neue Kultur der Risikoanalyse und des Risikomanagements angemahnt. Die Entwicklung »koordinierter Maßnahmen zur Prävention, Erkennung und Eindämmung von Störungen aller Art und zur entsprechenden Reaktion«[81] müsse als eine gleichzeitig globale, europäische und einzelstaatliche Herausforderung verstanden werden. Damit Angriffen aus Drittstaaten wirkungsvoller begegnet werden könne, müsse die Europäische Agentur für Netz- und Informationssicherheit (ENISA) modernisiert und verstärkt werden. Außerdem müssten die nationalen IT-Notfalldienste (CERT) zweckmäßiger koordiniert werden.[82] Auch in der Kommissionsmitteilung zur Strategie der inneren Sicherheit wird verlangt, neue CERTs aufzubauen und bestehende zu verbessern.[83] Es gelte, ein Europäisches Informations- und Warnsystem (European Information Sharing and Alert System, EISAS) für Angriffe auf kritische Infrastrukturen zu schaffen, zusammen mit der ENISA spezifische Notfallpläne in den Mitglied-

77 *EU-U.S. Summit 20 November 2010, Lisbon – Joint Statement*, MEMO/10/597, Brüssel, 20.11.2010.

78 *Cyber Security: EU and US Strengthen Transatlantic Cooperation in Face of Mounting Global Cyber-security and Cyber-crime Threats*, MEMO/11/246, Brüssel, 14.4.2011.

79 Ein Beispiel hierfür ist die Erklärung von Cecilia Malmström, *The EU Internal Security Strategy – What Does It Mean for the United States?* Discussion Organised by the Center for Transatlantic Relations, Speech/10/739, Washington, D.C., 8.12.2010.

80 Europäische Kommission, *Mitteilung über den Schutz kritischer Informationsinfrastrukturen* [wie Fn. 14].

81 Rat der Europäischen Union, *Schutz kritischer Informationsinfrastrukturen – »Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit« – Annahme der Schlussfolgerungen des Rates*, 10299/11, Brüssel, 19.5.2011, S. 2.

82 European Network and Information Security Agency (ENISA), *ENISA auf Deutsch*, <http://www.enisa.europa.eu/media/enisa-auf-deutsch>.

83 Vgl. auch Council of the European Union, *Draft Council Conclusions on the Development of the External Dimension of the European Programme for Critical Infrastructure Protection*, 10662/11, Brüssel, 27.5.2011.

staaten zu erarbeiten und regelmäßige Notfallübungen abzuhalten.

In der Übung Cyber Europe 2010[84] erwies sich, dass die EU auf externe Onlinebedrohungen nur schlecht reagieren kann, weil interne Strukturen in kleineren Mitgliedstaaten ungenügend entwickelt und die Kompetenzen der EU uneinheitlich geregelt sind.[85] Innere Strukturprobleme entpuppen sich auf diese Weise schnell als Verwundbarkeiten gegenüber Bedrohungen von außen. Oder anders ausgedrückt: Innenpolitik wird sicherheitspolitisch relevant. Unzulängliche Regulierung wirkt sich unmittelbar schädlich auf andere Staaten aus.

Versicherheitlichung

Eine weitere offensichtliche Entwicklung ist die zunehmende Versicherheitlichung der innenpolitischen EU-Agenda. Das Ziel, einen gemeinsamen »Raum der Freiheit, der Sicherheit und des Rechts« aufzubauen, wird von den Mitgliedstaaten und der Kommission unter dem Eindruck der neuen Bedrohungslagen immer einseitiger zugunsten sicherheitspolitischer Maßnahmen interpretiert.[86] Der Europäische Rat forderte in seinem Stockholmer Programm »eine umfassende Unionsstrategie der inneren Sicherheit«,[87] bei der datenschutzrechtliche Fragen nur noch untergeordnete Bedeutung haben. Die Kommission reagierte auf das Programm denn auch nicht mit einem weitreichenden Aktionsplan zur Ausdehnung von Bürgerfreiheiten und -rechten, sondern mit einer Mitteilung, in der sie schwere und organisierte Kriminalität, Cyberkriminalität, Terrorismus, Grenzsicherung und Katastrophenabwehr als akuteste gemeinsame Probleme benannte.[88] Die Cybersicherheitspolitik müsse zwar ebenfalls »auf gemeinsamen Werten aufbauen [...], u.a. auf dem Grundsatz der Rechtsstaatlichkeit und der Achtung der Grundrechte«, doch wird diesem Punkt inhaltlich kaum Rechnung getragen. Ausführlich geht die Kommission auf die sicherheitspolitischen Herausforderungen und Zielsetzungen sowie auf notwendige Maßnahmen ein. Sie sagt jedoch nichts darüber, dass parallel ein umfassendes Regelwerk geschaffen werden müsste, das die informationellen Grundrechte der Bürger gegenüber expansiven staatlichen Eingriffen schützt. Auch im angehängten Katalog der vorgesehenen Maßnahmen findet sich nichts zu diesem Thema.

Angesichts der wahrgenommenen Cyberbedrohungen verlagert sich die politische Schwerpunktsetzung weg von Freiheit und hin zur Sicherheit. Auch der Europäische Datenschutzbeauftragte beklagt, dass »bestimmte Maßnahmen, die aus den Zielen der ISS abgeleitet werden, die Risiken für den Schutz der Privatsphäre und den Datenschutz von Personen erhöhen«.[89]

Bemerkenswert ist weiterhin, dass sich die Dynamik der europäischen Sicherheitspolitik immer mehr auf administrative Akteure konzentriert. Bei der Umsetzung der Strategie zur Inneren Sicherheit sollen vorrangig die Agenturen der EU gleichberechtigt an der Seite der EU-Organe wie EP, Kommission und Rat sowie der Mitgliedstaaten handeln.[90] In der EU befassen sich ENISA, Europol, European Police College (CEPOL), European Maritime Safety Agency (EMSA) und der Europäische Auswärtige Dienst (EAD) mit Fragen der Cybersicherheit und -kriminalität. Ende März 2012 hat die EU-Kommission zudem angeregt, ein Zentrum für Cyberkriminalität einzurichten.[91] Es soll bei Euro-

84 Vgl. Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko u.a.: Cyber-Übungen der Europäischen Union, der USA und die deutsche Beteiligung*, Drucksache 17/7578, 2.11.2011.

85 Europäische Kommission, *Mitteilung über den Schutz kritischer Informationsinfrastrukturen* [wie Fn. 14].

86 Vgl. hierzu Madalina Busuioc/Deirdre Curtin, *Die EU-Strategie der inneren Sicherheit, der EU-Politikzyklus und die Rolle der (RSFR-)Agenturen: Perspektiven, Stolpersteine und Auswege*, Studie im Auftrag des Europäischen Parlaments, PE453.185, Brüssel 2011; Europäische Kommission, *Mitteilung der Kommission: Eine Strategie für die Außendimension des Raums der Freiheit, der Sicherheit und des Rechts*, KOM(2005) 491 endg., Brüssel, 12.10.2005; Myriam Dunn Cavelty/Kristian Søby Kristensen, »Introduction«, in: dies. (Hg.), *Securing »the Homeland«. Critical Infrastructure, Risk, and (In)Security*, London: Routledge, 2008.

87 »Das Stockholmer Programm – ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger«, in: *Amtsblatt der Europäischen Union*, C 115, 4.5.2010, S. 1, 17.

88 Vgl. Europäische Kommission, *Mitteilung der Kommission an das Europäische Parlament und den Rat vom 22. November 2010 – EU-Strategie der inneren Sicherheit. Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa*, KOM(2010) 673 endg., Brüssel, 22.11.2010.

89 »Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament und den Rat – ›EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa‹«, in: *Amtsblatt der Europäischen Union,* C 101, 1.4.2011, S. 6, 9.

90 Siehe hierzu grundlegend Deirdre Curtin, *Executive Power of the European Union. Law, Practices, and the Living Constitution*, New York 2009.

91 European Commission, Communication from the Commission to the Council and the European Parliament, *Tackling*

pol angesiedelt und zur Zentralstelle für die Bekämpfung der Cyberkriminalität in der EU erweitert werden. Mit seiner Hilfe könnten Mitgliedstaaten und Organe der EU operationelle und analytische Kapazitäten für Ermittlungen aufbauen und die Zusammenarbeit mit internationalen Partnern ausweiten. Ferner sollen bis 2013 in Absprache mit der Justizbehörde der EU (Eurojust) und Europol Ausbildungs- und Exzellenzzentren ausgebaut werden, die eng mit Hochschulen und Industrie kooperieren.[92] Gleichzeitig ist eine Marginalisierung des Europäischen Parlaments nicht zu übersehen:[93] »Es mag unglaublich erscheinen, doch in den wichtigsten strategischen Papieren, die bisher vom Europäischen Rat, vom Rat und von der Kommission angenommen wurden, wird das Europäische Parlament offensichtlich schlichtweg übergangen. War ein solches Versäumnis schon vor dem Inkrafttreten des Vertrags von Lissabon befremdend, so ist es nun [...] umso unerklärlicher.«[94]

Die legislative Schwerpunktverlagerung der EU betrifft auch den Datenschutz. Da die EU in puncto individuelle Freiheitsrechte alles andere als regulatorischen Eifer an den Tag legt, gibt es in Europa noch immer »ein[en] »Flickenteppich von Datenschutzvorschriften«.[95] Dort, wo die EU regulierend tätig wird, bewirken ihre Maßnahmen eher, dass der individuelle Grundrechtsschutz abgebaut statt gestärkt wird. Die Richtlinie 2006/24 zur Vorratsdatenspeicherung ist ein typisches Beispiel.[96] Sie verpflichtet jeden EU-Mitgliedstaat dazu, die Telefonverbindungen sämtlicher Bürger aufzeichnen zu lassen. Um etwaige strafrechtliche Ermittlungen zu erleichtern, soll nachvollziehbar sein, wer mit wem in den letzten sechs bis 24 Monaten per Telefon, Mobiltelefon oder E-Mail in Verbindung gestanden hat. Bei mobilen Telefonaten, SMS und Smartphone-Nutzung muss auch der jeweilige Standort des Benutzers festgehalten werden. Die Vorratsspeicherung von Internetkennungen (IP-Adressen) soll es in Verbindung mit anderen Informationen ermöglichen, Nutzer zu identifizieren. Diese tief in die informationelle Selbstbestimmung eingreifende Richtlinie hätte eigentlich bis zum 15. September 2007 von allen EU-Staaten in innerstaatliches Recht umgesetzt werden sollen. Deutschland hatte der EU-Kommission im Januar 2008 den Katalog seiner entsprechenden Maßnahmen übermittelt. Derzeit ist die Regelung aber ausgesetzt, denn das Bundesverfassungsgericht erklärte sie Anfang März 2010 für verfassungswidrig. Nach Ansicht der Karlsruher Richter verstieß sie gegen das grundgesetzlich garantierte Post- und Fernmeldegeheimnis. Hier deutet sich eine neue Konfliktlinie zwischen der EU-Kommission und einem dem Grundgesetz verpflichteten Bundesverfassungsgericht an.

Privatisierung von Regieren

Auf der globalen Ebene lässt sich beobachten, dass private Akteure immer stärker in die Cyberpolitik einbezogen werden. Dieser Prozess findet auf der europäischen Ebene seine Fortsetzung, abzulesen an den europäischen Strukturen der Cybersicherheitspolitik. Udo Helmbrecht, Direktor der ENISA, forderte, neben den Mitgliedstaaten auch private Akteure an der Arbeit der Agentur zu beteiligen. Hierzu gehören Cybersicherheitsübungen, öffentlich-private Partnerschaften für Netzwerkstabilität, Wirtschaftsanalysen und Risikobewertungen sowie Kampagnen zur Sensibilisierung der Bevölkerung und des Mittelstandes gegenüber den Gefahren des Internets: »Alle Sicherheitsbeauftragten müssen aus diesem Grund enger zusammenarbeiten und Strategien entwickeln, die besser sind und in engerer Kooperation eingesetzt werden.«[97] Ferner hat die ENISA einen ausführlichen

Crime in Our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, Brüssel, 28.3.2012.

92 Vgl. Europäische Kommission, *EU-Strategie der inneren Sicherheit* [wie Fn. 88].

93 Siehe dazu grundlegend Aidan Wills/Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Studie im Auftrag des Europäischen Parlaments, PE453.207, Brüssel 2011.

94 Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, *Arbeitsdokument 2 über die Strategie der inneren Sicherheit der Europäischen Union*, Berichterstatterin: Rita Borsellino, PE458.598v01-00, Brüssel 2011, S. 4.

95 Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for EU-Internal Information Exchange*, Dissertation, Luxemburg 2011, S. 226.

96 »Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG«, in: *Amtsblatt der Europäischen Union*, L 105, 13.4.2006.

97 Vgl. ENISA, *EU Agency Analysis of »Stuxnet« Malware: a Paradigm Shift in Threats and Critical Information Infrastructure Protection*, Presseerklärung, 7.10.2010, <http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1> (Zitat bei Matthias Monroy, »EU fürchtet Angriffe auf Informationssysteme«, in: *Heise Online* –

Leitfaden für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor formuliert, die sogenannte Partnerschaft für Robustheit (European Public-Private Partnership for Resilience, EP3R). Sie beruht auf einem gegenseitigen Interesse: Die EU und die nationalen Regierungen möchten von privatem Sachverstand profitieren, die beteiligten Unternehmen erhoffen sich effektivere Gesetze sowie wirksameren Schutz vor Spionage- und anderen Angriffen.

Die EU will mit Internetanbietern und gemeinnützigen Organisationen noch intensiver zusammenarbeiten und gemeinsam gegen illegale Internetinhalte vorgehen, wie etwa Aufrufe zum Terrorismus. Hierzu sollen gemeinsame Leitlinien für Anmelde- und Löschverfahren vereinbart werden. Über eine eigene Internetplattform (Contact Initiative against Cybercrime for Industry and Law Enforcement, CICILE) plant sie zudem, Kontakte zu interessierten Kreisen zu knüpfen.[98] Auch Europol verstärkt seine Kooperation mit privaten Unternehmen, beispielsweise mit ICPSA.

Nicht zuletzt einigten sich die Abgeordneten des EP-Innenausschusses im Frühjahr 2012 darauf, dass IT-Anbieter künftig stärker in die Pflicht genommen werden sollten. Der Ausschuss verlangt, dass Unternehmen ihre IT-Systeme sorgfältiger vor Angriffen schützen und sanktioniert werden sollen, wenn sie Mindestsicherheitsstandards missachten. Ferner sind künftig in der gesamten EU empfindliche Strafen für Hackerangriffe auf IT-Netzwerke vorgesehen. Unternehmen sollen zu vorbeugenden Schutzmaßnahmen und zur Zusammenarbeit mit der Polizei verpflichtet werden. Der Innenausschuss hat sich auch dafür ausgesprochen, solche kriminellen Angriffe konsequent in der ganzen Union zu bestrafen. Insgesamt soll die Zusammenarbeit sowohl von Behörden untereinander als auch von öffentlicher und privater Seite verbessert werden.[99]

Telepolis, 11.10.2010).

98 Siehe Council of the European Union, *Council Conclusions Concerning an Action Plan to Implement the Concerted Strategy to Combat Cybercrime*, 15569/08, Brüssel, 26.4.2010; Council of the European Union, *Draft Council Conclusions on an Action Plan to Implement the Concerted Strategy to Combat Cybercrime*, 5957/2/10, Brüssel, 25.3.2010, <http://www.statewatch.org/news/2010/mar/eu-council-revised-cyber-crime-conlcusions-5957-rev2-10.pdf> (eingesehen am 22.3.2012).

99 Monika Hohlmeier, *EU-Strafrecht: Cyber-Angriffe sind kein Kavaliersdelikt/Konsequente Strafen gegen Hacker-Attacken/Unternehmen müssen ihre IT-Systeme besser schützen/EP-Innenausschuss zu neuer EU-Richtlinie*, Pressemitteilung, 27.3.2012, <http://www.monika-hohlmeier.de/eu-strafrecht-cyber-angriffe-sind-kein-kavaliersdelikt-konsequente-strafen-gegen-hacker-attacken-unternehmen-muessen-ihre-it-systeme-besser-schuetzen-ep-innenausschuss-zu-neuer-eu-richtlinie/> (eingesehen am 8.4.2012); siehe auch Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, Replacing Council Framework Decision 2005/222/JHA*, 10751/11, Brüssel, 30.5.2011.

Leitlinien für eine europäische Cybersicherheitspolitik

Wenn diese allgemeinen Entwicklungen zusammengenommen interpretiert werden, entsteht das Bild einer institutionellen Ordnung, die in vielerlei Hinsicht von dem abweicht, was wir als demokratisch verstehen. Es ist eine Architektur, die sich über mehrere Ebenen verteilt, wesentlich auf dem Input privater Unternehmen aufbaut und keine sinnvolle Trennung zwischen Innen(politik) und Außen(politik) mehr zulässt. Alle diese Ebenen und Dimensionen von Regulierung sind in einer netzwerkartigen Struktur miteinander verwoben (siehe Abschnitt »Zusammenfassung«). Hieraus erwachsen eine Reihe demokratiepraktischer Probleme, die bei Regulierungsvorschlägen berücksichtigt werden sollten (siehe Abschnitt »Empfehlungen«).

Zusammenfassung

Die globale Regulierung des Internets ist jenseits konstitutioneller Überlegungen in einem als spontan zu bezeichnenden Prozess entstanden und dürfte sich auch zukünftig genau so weiterentwickeln. Sie emergiert eher, als dass sie Produkt eines wohldurchdachten Plans wäre. Wir haben es mit einer politischen Struktur zu tun, die auf den Prinzipien Kooperation, Koordination und Kooptation basiert und keinen dominanten einheitlichen Akteur kennt, der ihre Funktionslogik maßgeblich beeinflussen würde. Weder die USA noch die EU oder eine andere internationale Organisation sind eigenständig in der Lage, die globale Cybersicherheitspolitik entscheidend zu prägen, ohne auf die jeweils anderen Ebenen Rücksicht nehmen zu müssen.

Die europäische Cybersicherheitspolitik ist Teil einer Mehrebenen- und Multistakeholder-Struktur, in der übergreifende Konsensbildungsprozesse gestaltet werden müssen und in der privates Expertentum ausschlaggebend ist. Fachleute aus privaten Unternehmen und Organisationen können hier wahrscheinlich zum ersten Mal Sicherheitspolitik mitgestalten. Bisher war dies nur in weniger sensiblen Funktionsbereichen des Staates der Fall, wie Wirtschaftspolitik, Umweltpolitik oder Daseinsvorsorge. Ohne die Gefahren zu bagatellisieren, die aus einseitiger Einflussnahme auf Politik erwachsen: Dieser Prozess lässt sich auch optimistisch als beginnende Demokratisierung der Sicherheitspolitik verstehen.

Über die europäischen Agenturen oder transnationale nichtstaatliche Institutionen werden die Interessen privater Akteure dort in den politischen Prozess einbezogen, wo diese über relevantes Wissen verfügen. Es ist davon auszugehen, dass ihr Wissensvorsprung es ihnen in vielen Fällen ermöglicht, die politische Agenda wesentlich mitzubestimmen. Weder die Kommission noch der Europäische Rat besitzen in dieser neuen Struktur die umfassende Fähigkeit zur Prozessgestaltung und Agendasetzung. Vielmehr handelt es sich um eine tief gestaffelte Mehrebenenpolitik, in der Wissen und Autorität weit verteilt sind und breite Abstimmungsprozesse zwischen Stakeholdern mindestens so wichtig sind wie Prozesse der Mehrheitsbildung. Außer im Mitbestimmungsverfahren spielt das EP eher eine untergeordnete Rolle.

Transparenz und Rechenschaftspflicht lassen in fast allen beschriebenen Bereichen sehr zu wünschen übrig. Akteure ohne spezifisches Wissen oder politische Autorität bleiben auf internationaler, europäischer und nationaler Ebene außen vor. Vor allem die nationalen Parlamente sind auf allen drei Ebenen bestenfalls Nebendarsteller. Sie sind weder auf der europäischen Ebene präsent noch in die nationalen Verfahren der Gefahrenabwehr eingebunden. Angesichts ihrer zentralen Bedeutung für die Demokratie muss diese Abwesenheit als gravierendes Problem betrachtet werden. Zumindest auf nationaler und europäischer Ebene müssen daher erhebliche Anstrengungen unternommen werden, um Parlamente in die Lage zu versetzen, den europäischen Regelsetzungsprozess kompetent zu verfolgen und gut begründete Positionen zu entwickeln. Die derzeitige wissenschaftliche Ausstattung des Bundestages sowie des Europäischen Parlaments ist hierfür allerdings vollkommen unzureichend.

Empfehlungen

Wie ist die neue europäische Cybersicherheitsarchitektur zu bewerten? Welche Maßstäbe können

gewährleisten, dass sie demokratischen Ansprüchen genügt? Die Kommission hat in ihrem Weißbuch zum guten Regieren[100] betont, dass sich politische Entscheidungsverfahren an den Kriterien Transparenz, Rechtsstaatlichkeit, Rechenschaftspflicht und Partizipation messen lassen müssen. Privat-öffentliche Partnerschaften in der Regelsetzung sind in diesem Kontext grundsätzlich dort zu begrüßen, wo sie gesellschaftliches Wissen und staatliche Autorität sinnvoll miteinander kombinieren. Verhindert werden muss jedoch, dass sogenannte diffuse Interessen organisationsschwacher Stakeholder, Anliegen informationeller Selbstbestimmung und breitere gesellschaftliche Teilhabe unberücksichtigt bleiben. Die Regulierung des Internets ist für viele Bereiche des politischen, ökonomischen und privaten Lebens so wichtig, dass sie nicht von Expertengremien hinter verschlossenen Türen gestaltet werden sollte. Gerade die Sicherheitspolitik muss sich diesem Thema intensiver zuwenden.

In der aktuellen politischen Debatte finden sich mindestens fünf konkrete Vorschläge, wie der Cyberspace sicherer gemacht werden könnte. Sie lassen sich anhand der oben genannten Kriterien bewerten:

Bewusstseinsbildung: Fast alle Institutionen und Personen, die mit Fragen der Sicherheit im Internet befasst sind, weisen nachdrücklich darauf hin, dass mehr gesellschaftliches und politisches Bewusstsein für die Gefahren von Cyberkriminalität und Cyberterrorismus geschaffen werden muss. Hierzu bedarf es eines hohen Maßes an Transparenz. Vertreter der Strafverfolgungsbehörden müssen gut ausgebildet und sowohl von der technischen Ausstattung als auch vom Know-how her in die Lage versetzt werden, Kriminellen und Terroristen Paroli zu bieten. Der Bundestag hat ebenso wie viele nationale Ministerien Gremien eingerichtet, um der Herausforderung zu begegnen. Auch die Sicherheitsdienste haben erste wichtige Schritte unternommen. Was im Hinblick auf die nötige Transparenz allerdings noch fehlt, ist der Informationsaustausch über Quantität und Qualität von Cyberangriffen, der zwischen Exekutive und Legislative und vor allem zwischen privaten Unternehmen und Sicherheitsbehörden stattfinden muss.

Verbesserung des Wissensstandes: Ähnlich wie in den USA gibt es in der EU derzeit eine unter Experten breit diskutierte Initiative, private Unternehmen darauf zu verpflichten, Cyberangriffe an die zuständigen staatlichen Stellen zu melden. Diesen Eingriff in die informationelle Selbstbestimmung von Unternehmen verteidigt die US-Regierung mit dem Argument der nationalen Sicherheit. Dem entgegen steht die Freiheit des Einzelnen oder des einzelnen Unternehmens, eigenständig darüber zu bestimmen, wem welche Informationen zugänglich gemacht werden. Hier handelt es sich um eine schwierige, kontroverse Abwägung hoher politischer Güter. Sie führt vor Augen, wie notwendig es ist, Fragen der Internetregulierung nicht nur in technischen Expertengremien zu besprechen, sondern in einem möglichst partizipativen Kontext unter Einschluss parlamentarischer Gremien.

Strafverfolgung: Über alle Fragen der Internetsicherheit wird immer wieder aus dem Blickwinkel der Abschreckung und damit der Verschärfung von Strafen debattiert. Es ist unbestritten, dass Angriffe auf kritische Infrastrukturen gegen die staatliche Sicherheit gerichtet sind und daher massiv geahndet werden müssen. Es besteht auch kein Zweifel daran, dass der Einbruch in eine Datenbank grundsätzlich genauso zu bewerten ist wie der Einbruch in ein Gebäude. Das deutsche Strafrecht bietet ausreichend Möglichkeiten, dies zu sanktionieren. Die internationale Koordinierung dagegen muss noch so weit global harmonisiert werden, dass rechtsfreie Räume oder Räume ohne Strafverfolgung vermieden werden. Der Rechtsstaat muss auch im Internet Gültigkeit haben.

Überarbeitung des Kriegswaffenkontrollgesetzes: Es sollte intensiver darüber nachgedacht werden, ob das Kriegswaffenkontrollgesetz modifiziert und auf Software ausgedehnt werden müsste. Malware kann für Angriffe auf andere Staaten bzw. deren Infrastrukturen verwandt werden. So betrachtet kann ein Computerprogramm ähnlich verheerende Wirkungen haben wie ein Panzer. Daher sollte auch der Export solcher Software überwacht werden, mit deren Hilfe autoritäre Systeme ihre Bevölkerung kontrollieren und oppositionelle Kommunikation unterbinden können. Unternehmen müssen Rechenschaft darüber ablegen, wohin und was sie exportieren.

Globaler Verhaltenskodex: Um Rechenschaftspflicht weltweit zu fördern, muss ein globaler Verhaltenskodex für den Cyberspace aufgestellt werden. Er sollte sowohl für Staaten als auch für nichtstaatliche Akteure wie Unternehmen und Individuen gelten und wesentliche Tatbestände definieren. Hierzu gehören der Angriff auf kritische Infrastrukturen, der Einbruch in fremde Datenbanken, der unerlaubte Zugriff auf private Daten und deren Verwendung sowie die priva-

100 Vgl. Kommission der Europäischen Union, *Europäisches Regieren. Ein Weißbuch*, KOM(2001) 428 endg., Brüssel, 25.7.2001.

te oder staatliche Spionage. Noch blockieren die USA Versuche, einen solchen Kodex zu formulieren. Für Staaten und Gesellschaften mit wenigen Ressourcen ist diese Blockade nur schwer hinzunehmen. Sie perpetuiert nicht nur die Freiheit der USA, nach eigenem Ermessen zu handeln, ohne dafür zur Verantwortung gezogen zu werden, sondern auch die Verwundbarkeit aller anderen Staaten.

Sollten all diese Maßnahmen nicht greifen oder gar nicht erst eingesetzt werden, werden die Rufe lauter werden, dass die Reichweite des Internets eingeschränkt werden müsse. Schon heute mehren sich die Stimmen für eine »Entnetzung«. Die Forderungen beschränken sich nicht auf Schritte, mit denen sicherheitsrelevante Daten vom Internet abgekoppelt werden. Verlangt wird auch, Informationen zurückzuhalten, deren Zugänglichkeit im öffentlichen Interesse ist. Im Extremfall könnte die Strategie der Entnetzung dem Versuch dienen, nationale Autarkie zurückzugewinnen. Iran etwa strebt danach, sein nationales Netz weitgehend vom globalen Internet zu trennen, um die Gefahr von Angriffen auf seine (Atom-)Industrie zu verringern. Gleichzeitig sollen derartige Maßnahmen auch dissidente Kommunikationen regulieren und die eigenen Bürger daran hindern, weiter an der kritischen Debatte teilzunehmen. Ähnliches lässt sich in China beobachten.

Spielarten der Entnetzung und der Förderung nationaler Autarkie sind ausgesprochen heikle politische Instrumente und potentielle Bedrohungen der Freiheit. Umso notwendiger ist es, in den fünf hier skizzierten Feldern voranzukommen.[101] Die vorgeschlagenen Methoden können nur dann Erfolg haben, wenn sie private Akteure einbinden. Zudem dürfen regulative Strategien wie die geplante EU-Strategie zur Cybersicherheit nicht nur an vermeintlichen Effektivitätskriterien ausgerichtet werden. Sie müssen sich an Grundsätzen messen lassen, die für die Demokratie konstitutiv sind, nämlich Transparenz, Rechtsstaatlichkeit, Rechenschaftspflicht und Partizipation.

101 Wenn Staaten sich weigern, präventiv Normen festzulegen, setzen sie das ganze Netz einem Risiko aus. Siehe Bruce Schneier, »Cyberwar Treaties«, *Schneier on Security* (Blog), 14.6.2012, <http://www.schneier.com/blog/archives/2012/06/cyber-war_treati.html?utm_medium=twitter&utm_source=twitterfeed> (eingesehen am 26.6.2012).

Abkürzungsverzeichnis

ACTA	Anti-Counterfeiting Trade Agreement
AFET	Committee on Foreign Affairs/ Commission des affaires étrangères (EP)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCD COE	Cooperative Cyber Defence Centre of Excellence
CDMA	Cyber Defence Management Authority
CDU	Christlich Demokratische Union
CEPOL	European Police College
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIRP	Committee for Internet-Related Policies (VN)
COSI	Standing Committee on Operational Cooperation on Internal Security
CSU	Christlich-Soziale Union
EAD	Europäischer Auswärtiger Dienst
EISAS	European Information Sharing and Alert System
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EP	Europäisches Parlament
EP3R	European Public-Private Partnership for Resilience
EU	Europäische Union
FDP	Freie Demokratische Partei
FIRST	Forum of Incident Response and Security Teams
FS-ISAC	Financial Services – Information Sharing and Analysis Center
ICANN	Internet Corporation for Assigned Names and Numbers
ICSPA	International Cyber Security Protection Alliance
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGCI	Interpol Global Complex for Innovation
IGF	Internet Governance Forum
IP	Internetprotokoll
IT	Information Technology
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
LIBE	Committee on Civil Liberties, Justice and Home Affairs (EP)
Nato	North Atlantic Treaty Organization
NCAZ	Nationales Cyber-Abwehrzentrum
NCIRC TC	Nato Computer Incident Response Capability – Technical Centre
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OPC	Observatory for the Prevention of Crime
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PSK	Politisches und Sicherheitspolitisches Komitee
QANGO	Quasi-autonomous Non-governmental Organization

RFC	Request for Comments
RiR	Regional Internet Registry
SMS	Short Message Service
USA	United States of America
VN	Vereinte Nationen
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WSIS	World Summit on the Information Society