Zwischen Strafverfolgung und nachrichtendienstlicher Analyse. Konsequenzen aus der Europäisierung der Cybersicherheitspolitik für Deutschland

*Cathleen Berger**

„In Ländern außerhalb der EU kann es auch vorkommen, dass Regierungen den Cyberraum zur Überwachung und Kontrolle ihrer Bürger missbrauchen. Die EU kann solchem Missbrauch entgegenwirken, indem sie die Freiheit des Internets unterstützt und die Wahrung der Grundrechte im Internet gewährleistet."[1]

Mit diesem Leitbild begründet die Europäische Union in ihrer Cybersicherheitsstrategie vom Februar 2013, warum weiteres Engagement gefördert und ein neuer Maßnahmenkatalog vorgeschlagen wird. Die Cybersicherheitsstrategie trägt als wichtiges Element zur Entwicklung einer gemeinsamen Cybersicherheitspolitik bei. Diese Entwicklung ist politisch interessant, weil die Fragen der Cybersicherheit dank der Spionageprogramme Prism, Tempora oder X-Keyscore in aller Munde sind,[2] und zudem wissenschaftlich neu und spannend, weil die Union in diesem Politikfeld nur bedingt über eigene Kompetenzen verfügt. Während sie für die Regulierung des Wettbewerbs innerhalb des Binnenmarkts – folglich auch des digitalen Binnenmarkts – ausschließliche Zuständigkeit besitzt,[3] teilt sie sich die Zuständigkeit für den Raum der Freiheit, der Sicherheit und des Rechts mit den Mitgliedstaaten.[4] In Fragen des auswärtigen Handelns oder der Gewährleistung der öffentlichen Ordnung kann sie allenfalls beratend auftreten, nicht aber hierarchisch eingreifen. Für die Formulierung einer effektiven Cybersicherheitspolitik ist es aber notwendig, all diese Bereiche zu berücksichtigen.

Der Kompetenzmix wirkt sich in zwei Richtungen aus. Zum einen hat er Auswirkungen auf die Entstehung europäischer Politik (Integration), da er in diesem Zusammenhang vor allem das Handeln der Europäischen Kommission bestimmt. Zum anderen wirkt sich der europäische Politikgestaltungsprozess auf die nationalen Strukturen und Politiken aus (Europäisierung). Selbstverständlich sind diese Prozesse – Integration und Europäisierung – miteinander verflochten. Um die Konsequenzen sinnvoll einordnen zu können, ist es jedoch analytisch notwendig, die Prozesse voneinander zu trennen.[5]

---

* Cathleen Berger, M.A., Mag., Forschungsassistentin, Stiftung Wissenschaft und Politik, Berlin.

1 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Cybersicherheitsstrategie der EU – ein offener, sicherer und geschützter Cyberraum, JOIN (2013) 1, hier S. 3.

2 Siehe zum Beispiel: Daniela Kietz/Johannes Thimm: Zwischen Überwachung und Aufklärung. Die amerikanische Debatte und die europäische Reaktion auf die Praxis der NSA, Stiftung Wissenschaft und Politik: SWP-Aktuell 51/2013.

3 Art. 3 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).

4 Art. 4 Abs. 2 Lit. j AEUV.

5 Vergleiche hierzu Katrin Auel: Europäisierung nationaler Politik, in: Hans-Jürgen Bieling/Marika Lerch (Hrsg.): Theorien der europäischen Integration, Wiesbaden 2006, S. 293-318, hier S. 298 sowie Kevin Featherstone: Introduction: In the Name of 'Europe'?, in: Kevin Featherstone/Claudio M. Radaelli (Hrsg.): The politics of Europeanisation, Oxford 2003, S. 3-26, hier S. 19.

Dieser Beitrag konzentriert sich auf den Europäisierungsprozess und widmet sich daher der Rückwirkung der europäischen Regelungen im Politikfeld Cybersicherheit auf die Bundesrepublik Deutschland. Die Frage lautet: Welche sicherheitspolitischen Veränderungen werden innerhalb Deutschlands durch europäische Regelungen zur Cybersicherheit ausgelöst?

Aufgrund des Kompetenzmixes kann nur bedingt steuernd eingegriffen werden, sodass insbesondere Mechanismen der horizontalen Kooperation betrachtet werden müssen. Daher wird auf den Ansatz des ‚soft framing' zurückgegriffen.[6] Horizontale Kooperation meint die Annäherung von Ideen, Abstimmungsprozesse und Konsensfindung. ‚Soft framing' beschreibt den Mechanismus, über welchen eine solche Kooperation erreicht werden kann. Die Analyse umfasst zwei Dimensionen: das Objekt und das Ausmaß der Europäisierung. Cybersicherheit als Objekt ist im Bereich der ‚public policy' anzusiedeln, da es nicht um Strukturen, sondern Politikgestaltung geht. Das Ausmaß kann theoretisch vier Ausprägungen annehmen: Rückbau, Stillstand, Absorption und Transformation, wobei zum Beispiel Stillstand bedeutet, dass sich kein Europäisierungseinfluss beziehungsweise kein Wandel in der Politikgestaltung nachzeichnen lässt und Transformation eine Veränderung der fundamentalen Logik des politischen Handelns bedeuten würde.[7]

Die Europäische Union kann über vertikale wie horizontale Impulse Einfluss auf die nationale Politikgestaltung nehmen. Grundsätzlich gelten dabei Richtlinien und Verordnungen als vertikale Instrumente. Während Koordinierung, Diffusions-, Lern- und Sozialisierungsprozesse als horizontale Instrumente verstanden werden.[8] Auf horizontaler Ebene greift die Europäische Union also nicht hierarchisch in nationale Politikgestaltungsprozesse ein, sondern stellt Lösungen für Probleme bereit, die dann in die nationale Debatte eingebracht werden. Die Union fungiert dann als Arena, in der Ideen reifen und Konzepte entwickelt werden. In den Worten Claudio Radaellis wird Europäisierung folglich definiert als: „Processes of (a) construction, (b) diffusion, and (c) institutionalization of formal and informal rules, procedures, policy paradigms, styles, ‚ways of doing things', and shared beliefs and norms which are first defined and consolidated in the making of EU public policy and politics and then incorporated in the logic of domestic discourse, identities, political structures, and public policies."[9]

Die These lautet, dass es im Bereich der Cybersicherheit zu einer schrittweisen Absorption kommt. Das heißt, die Union gibt für dieses neue Politikfeld Impulse vor, definiert Mittel und konsolidiert Lösungen. Die Gewohnheit zur Koordination in anderen Politikfeldern regt

6 Für die Erklärung positiver Integration: Tanja Börzel: Institutional Adaptation to Europeanization in Germany and Spain, in: Journal of Common Market Studies 4/1999, S. 573-596; Tanja Börzel/Thomas Risse: Conceptualizing the Domestic Impact of Europe, in: Kevin Featherstone/Claudio M. Radaelli (Hrsg.): The Politics of Europeanization, Oxford 2003, S. 57-80; exemplarisch für die Erklärung negativer Integration: Christoph Knill/Dirk Lehmkuhl: The National Impact of European Union Regulatory Policy: Three Europeanization Mechanisms, in: European Journal for Political Research 2/2002, S. 255-280; für soft framing vergleiche: Auel: Europäisierung nationaler Politik, 2006, S. 306.

7 Ebenda, S. 299. Sie verwendet die Begriffe Retrenchment, Inertia, Absorbtion und Transformation.

8 Ebenda, S. 301.

9 Claudio Radaelli: The Europeanization of Public Policy, in: Kevin Featherstone/Claudio M. Radaelli (Hrsg.): The Politics of Europeanization, Oxford 2003, S. 27-56, hier S. 30. Um diese Prozesse zu untersuchen, werden in erster Linie offizielle Dokumente der Organe und Institutionen der Europäischen Union zu Rate gezogen. Die Kommission darf als Initiativorgan zum Beispiel Richtlinienvorschläge unterbreiten und prägt vor allem über Strategiedokumente die Politikformulierung der Europäischen Union. Berichte von Einrichtungen wie Europol geben Aufschluss über die Institutionalisierung von formalen und informellen Regeln und Prozeduren. Diese werden anschließend in Beziehung zu den Maßnahmen der Bundesrepublik gesetzt, um die Rückwirkung des europäischen Politikgestaltungsprozesses nachzuzeichnen.

einen weiteren Sozialisierungsprozess an, sodass ein Anpassungsdruck entsteht, der die deutsche Haltung nachhaltig verändert. Im Folgenden wird zunächst die Problematik Cybersicherheit eingehender beleuchtet. Danach werden die Politiken und Maßnahmen im Bereich der Cybersicherheit auf europäischer Ebene vorgestellt, bevor deren Rückwirkung auf den Umgang mit Cybersicherheit innerhalb Deutschlands untersucht wird. Der Schlussteil greift die Konsequenzen aus diesem Politikgestaltungsprozess auf und plädiert für eine offenere und intensivere Auseinandersetzung mit den Folgen.

Cyberraum, Cybersicherheit, Cyberkriminalität

Wenn es darum geht, eine Cybersicherheitspolitik zu formulieren, sollte Klarheit darüber bestehen, was unter Cybersicherheit verstanden wird. Hier trifft man schon auf die erste Hürde. Cybersicherheit kann heißen Sicherheit *im* Cyberraum oder Sicherheit *des* Cyberraums. Neben der Frage, ob der Raum als solcher oder das Handeln innerhalb dieses Raumes gesichert werden soll, stellt sich die Frage nach der Beschaffenheit des Cyberraums. Die Meinungen, wie weit oder wie eng dieser Begriff gefasst wird, gehen auseinander. Eine mögliche Definition lautet: „Cyberspace is defined as ICT [information and communication technology] systems, networks and the information contained within these systems and networks, whether online or offline."[10] Das Internet, Telekommunikation, Datenpakete, IT-Infrastrukturen, Kommunikationsnetzwerke – all dies und mehr kann so dem Cyberraum zugerechnet werden. In anderen Definitionen wird nur auf einzelne dieser oder auch zusätzliche Elemente, wie die Bedeutung von Raum und Tiefe, zeitlicher und sozialer Dimension, Bezug genommen.

Die Unklarheiten bezüglich Reichweite, Beschaffenheit und technischer Ausstattung des Cyberraums führen schnell zu Unklarheiten in der Bedeutung von Sicherheit beziehungsweise den Formen von Kriminalität und Attacken im Cyberraum. Einerseits ist dies unterschiedlichen Interessenlagen von Staaten geschuldet, andererseits aber auch der Tatsache, dass der wissenschaftliche Diskurs zum Thema noch relativ jung ist. Bisher fand eine Auseinandersetzung mit Cybersicherheitsfragen vor allem im anglo-amerikanischen Raum statt, die erst allmählich von europäischen Wissenschaftlern aufgegriffen wird.[11] In vielerlei Hinsicht handelt es sich bei diesen Beiträgen um ‚Foresight'-Literatur, die sich darum bemüht, Potenziale, Möglichkeiten und Formen (künftiger) Bedrohungen im Cyberraum abzuschätzen. Dies geschieht vor dem Hintergrund der stetig wachsenden Abhängigkeit von Gesellschaft, Staat und Wirtschaft von Informationssystemen und Infrastrukturen.[12] Darüber hinaus drehen sich die Cyberszenarien häufig um die Möglichkeiten und Gefahren eines Cyberkrieges.[13] Dabei wird der Cyberraum beispielsweise als fünfter Raum der Kriegsführung,

10 Sacha Tessier-Stall: The future of cybersecurity, in: The Hague Centre for Strategic Studies and TNO: Paper 4/2011, S. 9.

11 Vergleiche: Annegret Bendiek/Kathrin Ulmer: Cybersicherheit – Eine facettenreiche politische Herausforderung, Stiftung Wissenschaft und Politik: SWP-Zeitschriftenschau 3/2013; Jan Kuhn: Der Schutz kritischer Infrastrukturen. Unter besonderer Berücksichtigung von kritischen Informationsinfrastrukturen, Hamburg: Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle, Institut für Friedensforschung und Sicherheitspolitik, Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle: Working Paper 5/2005, S. 3; Tessier-Stall: The future of cybersecurity, 2011.

12 Ebenda, S. 16; Fred Schreier/Barbara Weekes/Theodor H. Winkler: Cyber Security: The Road Ahead, Geneva Centre for the Democratic Control of Armed Forces: DCAF Horizon 2015 Working Paper 4/2011.

13 Anstatt Vieler: Tim Maurer: Cyber norm emergence at the United Nations – an analysis of the activities at the UN regarding cyber-security, Cambridge 2011.

nach Land, See, Luft und All, kategorisiert.[14] Wie wahrscheinlich oder technisch durchführbar ein solch virtueller Krieg ist, soll hier außen vorbleiben. Im Fokus sollen die innere Dimension von Cybersicherheit und damit das Zusammenspiel von Strafverfolgung und Nachrichtendiensten in der Bekämpfung von Cyberkriminalität stehen.

Allerdings klaffen auch hier die Definitionen weit auseinander. Mal wird Cyberkriminalität auf wirtschaftliche Aspekte begrenzt, mal werden ökonomische und nicht-ökonomische Formen sowie solche, die das Internet zum Ziel haben, und solche, die das Internet als Medium nutzen, unterschieden. [15] In anderen Einteilungen werden die Kriminalitätsformen nach Gefahren- beziehungsweise Wirkungsstufen abgegrenzt.[16] Somit werden in der Literatur vornehmlich analytische Unterscheidungen vorgenommen und verschiedene Ausprägungen von Delikten unter dem Begriff Cyberkriminalität subsumiert, aber eine einheitliche Definition ist nicht erkennbar.[17]

Es lassen sich insbesondere vier Formen ableiten: erstens, organisierte Cyberkriminalität (vor allem finanzieller Betrug, Datenmissbrauch), zweitens, politisch motivierte Attacken (zum Beispiel Cyberspionage), drittens, Angriffe mit militärischem Potenzial (Stichworte sind Cyberkrieg und Cyberverteidigung) und viertens, Cyberterrorismus. Cyberterrorismus wird separat betrachtet, da es sich sowohl um politische oder ideologische Angriffe als auch um Angriffe mit militärischen Konsequenzen handeln kann.[18]

Diese weitgespannte Definition wirkt sich selbstverständlich auch auf den politischen Diskurs aus. Hier steht die Bestimmung von Straftatbeständen im Vordergrund, sodass meist nur auf einen Minimalkonsens für die zugrunde liegende Definition zurückgegriffen wird. Umstritten bleibt mitunter, ob eine solche Definition sich ausschließlich auf Delikte bezieht, die im Cyberraum begangen werden können oder auch auf solche, die durch die Gegebenheiten im Cyberraum erleichtert werden. In anderen Worten: Umfasst ein Verständnis von Cyberkriminalität nur Delikte wie Identitätsdiebstahl und digitale Erpressung oder auch Straftaten wie den spektakulären virtuellen Banküberfall, der im Mai 2013 aufgedeckt wurde? Im letzteren Fall hatte sich ein kriminelles Netzwerk Zugang zu Kreditkartenkonten in mindestens zwei großen Banken verschafft, deren Abhebungslimit erhöht und dann mithilfe von gefälschten Kreditkarten parallel in 26 Ländern an tausenden Bankautomaten Geld abgehoben. Das heißt, sie haben ihren Diebstahl virtuell vorbereitet, aber in der physischen Welt begangen.

Strafrechtlich steht außer Frage, dass es sich um eine kriminelle Handlung handelt, unklar ist nur, wo die Grenze von Cyberkriminalität gezogen wird: bei Straftaten *im* Cyberraum oder bei Straftaten *durch* den Cyberraum. In beiden Formen bietet die Selbstverständlichkeit mit der wir uns Online-Banking, E-Mail, Internetshopping oder der Standortbestimmung per GPS bedienen, eine breite Angriffsfläche für kriminelle Energien. Die Tatsache, dass kritische Infrastrukturen, wie Wasser- und Stromversorgung, zunehmend virtuell gesteuert wer-

14 Schreier/Weekes/Winkler: Cyber Security: The Road Ahead, 2011, S. 8.

15 Maurer: Cyber norm emergence at the United Nations, 2011, S. 3; Gregor Walter: Internetkriminalität. Eine Schattenseite der Globalisierung, Stiftung Wissenschaft und Politik: SWP-Studie 16/2008, S. 12.

16 Paul Cornish: Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, European Parliament, Directorate General for External Policies of the Union, PE 406.997, 2009, S. 7-16.

17 Vergleiche: Dominik Brodowski/Felix C. Freiling: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Forschungsforum Öffentliche Sicherheit: Schriftenreihe Sicherheit Nr. 4, Berlin 2011; Phil Williams/Timothy Shimeall/Casey Dunlevy: Intelligence Analysis for Internet Security, Contemporary Security Policy 2/2002, S. 1-38, hier S. 7.

18 Walter: Internetkriminalität, 2008, S. 22; James A. Lewis: Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats, Center for Strategic & International Studies, Dezember 2002, S. 1; Kuhn: Der Schutz kritischer Infrastrukturen, 2005, S. 22.

den, verstärkt diesen Eindruck zusätzlich. Aus politischer Sicht sollen daher alle Verständnisse – oder alle Formen – von Cyberkriminalität strategisch bekämpft werden, um sowohl Sicherheit *im* als auch *des* Cyberraums zu gewährleisten.[19]

Damit wird deutlich, dass das Problem der Definition oder sprachlichen Genauigkeit eng mit den zu ergreifenden Gegen- und Präventivmaßnahmen zusammenhängt. Gemeinsam ist den genannten Formen der Cyberkriminalität ihr transnationaler, ortsungebundener Charakter. Der Straftäter muss sich nicht an dem Ort aufhalten, an dem ein Delikt begangen wird. So könnte ein Spionageangriff auf italienische Regierungsserver über einen äthiopischen Netzbetreiber ausgeführt und von kolumbianischen Tätern initiiert werden, die sich in Malaysia aufhalten. Hinzu kommt, dass finanzieller Betrug eher von privaten, wenn auch organisierten, Tätern begangen wird. Ihnen wird strafverfolgend mit Mitteln der inneren Sicherheit begegnet. Spionageangriffe auf Regierungsdaten können dagegen durchaus von staatlicher Seite verübt werden. Hier klären Nachrichtendienste im Bereich der äußeren Sicherheit auf.

Ein Politikfeld, wie Cybersicherheit, dessen Rahmen über verschiedene Kompetenzbereiche hinweg gespannt ist, verlangt folglich umfassende Strategien und Maßnahmen. Mitunter werden so traditionelle Unterscheidungen zwischen innerer und äußerer Sicherheit, nachrichtendienstlichen und strafverfolgenden Aufgaben aufgeweicht. Dieser Diffusionsprozess wird auch seitens der europäischen Akteure, federführend von der Kommission, vorangetrieben. Diese hat den Kampf gegen Cyberkriminalität zu einem primären Anliegen der europäischen Sicherheitspolitik erklärt.[20]

Schrittweise Entwicklung einer Cybersicherheitspolitik der Europäischen Union

Die Kompetenzen sind im Politikfeld Cybersicherheit in der Europäischen Union auf mehrere Akteure verteilt. Mit Blick auf die Regulierung des digitalen Binnenmarktes ist die Europäische Kommission beispielsweise ermächtigt, vertikale Impulse zu geben. Diese Regulierung bezieht sich aber hauptsächlich auf wettbewerbsfördernde Komponenten und weniger auf die Gewährleistung eines sicheren Cyberraums. Diese Aufgabe ist vornehmlich im Bereich Justiz und Inneres und zwar insbesondere im Raum der Freiheit, der Sicherheit und des Rechts anzusiedeln. Aufgrund der geteilten Zuständigkeit von Europäischer Union und Mitgliedstaaten können vertikale Impulse hier nur eingeschränkt eingesetzt werden. Diese spielen unter anderem in der Regulierung des Schengenraums sowie in der Umsetzung des Europäischen Haftbefehls eine Rolle. Sie sind aber in der Formulierung einer Cybersicherheitspolitik zweitrangig. Im Wesentlichen kommen horizontale Impulse zum Einsatz, die ihr Fundament in den gemeinsamen Werten und einer gewissen Kongruenz von Überzeugungen finden.[21] Die Europäische Union stellt somit eine Arena dar, in der gemeinsame Ideen reifen können und Lösungsansätze entwickelt werden. So wird Cybersicherheit nicht zuletzt auch

19 Vergleiche: Neil Robinson/Luke Gribbon/Veronika Horvath/Kate Robertson: Cyber-security threat characterisation. A rapid comparative analysis, RAND Europe, 2013, hier S. VI.

20 Diese Prioritätensetzung wurde unter anderem von der Europäischen Kommission dargelegt und vom Rat der EU anschließend bestätigt. Vgl. Europäische Kommission: Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, KOM (2012) 140; Rat der EU: Entwurf von Schlussfolgerungen zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, Dok. 10603/12.

21 In der Europäisierungsliteratur wird unter anderem betont, dass für die Erzielung eines Konsenses in intergouvernementalen Politikfeldern, wie der Gemeinsamen Außen- und Sicherheitspolitik, ein besonderes Maß an Übereinstimmung von Ideen und Werten nötig ist. Vergleiche: Auel: Europäisierung nationaler Politik, 2006, S. 306.

in der Debatte um die Anwendung der Solidaritätsklausel nach Art. 222 AEUV sowie der Beistandsklausel aus Art. 42 Abs. 7 Vertrag über die Europäische Union (EUV) angeführt: Gelten Solidaritäts- und Beistandspflicht auch im Falle von Cyberangriffen und wenn ja, welche Formen fallen darunter und zu welchem Ausmaß müssen sie eintreten?[22] Zudem präsentiert sich das Europäische Parlament als aktiver Verfechter des Datenschutzes sowie einer verantwortungsvollen und freiheitlichen Nutzung des Cyberraums – Aspekte, die gezielt auf gemeinsame Werte und moralische Verpflichtungen rekurrieren.[23] Unterstützt wird die Entwicklung von gemeinsamen Vorstellungen durch einen gewissen Grad der Institutionalisierung, indem spezialisierte Einrichtungen, wie Europol oder die Europäische Agentur für Netz- und Informationssicherheit (ENISA), geschaffen und mit der Koordination bestimmter Aufgaben innerhalb des Politikfeldes beauftragt werden. In der Europäischen Union werden also Maßnahmen auf drei Ebenen ergriffen: strategisch, rechtlich und institutionell.[24] Die horizontalen Impulse der strategischen Ebene lassen sich über die Auswertung der offiziellen Dokumente aufzeigen. Auf der rechtlichen Ebene wird durch den Erlass von Richtlinien – wenn auch nur minimal – vertikal lenkend eingegriffen und auf der institutionellen Ebene werden Diffusions- und Lernprozesse institutionalisiert und durch gemeinsame Einrichtungen gesteuert. Das bedeutet auch, dass Einrichtungen wie Europol und ENISA die horizontalen Impulse unterstützen. Indem sie gemeinsame Übungen für die Mitgliedstaaten organisieren oder punktuell operative Erfolge erzielen, helfen sie den Prozess der Diffusion voranzutreiben.

(K)eine gemeinsame Definition

Ein erster Konsens für eine gemeinsame Definition von Delikten im Cyberraum konnte mit dem Übereinkommen über Computerkriminalität des Europarates (auch Budapester Konvention genannt) erzielt werden. Dieses wurde von allen Mitgliedstaaten der Europäischen Union unterzeichnet und trat am 1. Juli 2004 in Kraft. Es ist aber bislang nicht in allen Mitgliedstaaten ratifiziert (etwa in Griechenland, Irland, Luxemburg, Polen, Schweden und Tschechien).[25]

2011 unterbreitete die polnische Ratspräsidentschaft einen neuen Vorschlag für ein gemeinsames Glossar zur Cybersicherheit. Diese Initiative ist in ihrer Wortwahl jedoch sehr allgemein gehalten und definiert Cyberkriminalität schlicht als „an offence committed in

22 Sara Myrdal/Mark Rhinard: The European Union's Solidarity Clause: Empty Letter or Effective Tool?, Swedish Institute of International Affairs: UI Occasional Papers 2/2010, S. 9; Europäisches Parlament: Bericht über die EU-Klauseln über die gegenseitige Verteidigung und Solidarität: politische und operationelle Dimensionen (2012/2223(INI)), Berichterstatter Ioan Mircea Paşcu, A7-0356/2012.

23 Explizit unter anderem Europäisches Parlament: Entschließung zu Cyber-Sicherheit und Verteidigung, P7_TA(2012)0457 sowie zwei vom Parlament in Auftrag gegebene Studien: Cornish: Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, 2009; Didier Bigo et. al.: Fighting cyber crime and protecting privacy in the cloud, European Parliament, Directorate General for Internal Policies, PE 462.509, 2012.

24 In anderen Aufsätzen werden die Maßnahmen nach Funktion, nicht Ausgestaltung unterschieden. So versteht Gustav Lindstrom fast alle europäischen Maßnahmen als institutionell und mit Präventivfunktion. Vgl. Gustav Lindstrom: Meeting the Cyber Security Challenge, Geneva Centre for Security Policy: Geneva Papers 7/2012, S. 23.

25 Council of Europe: Covention on Cybercrime, Budapest 23.11.2001, abrufbar unter: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (letzter Zugriff: 18.11.2013). Der Status der Unterzeichnung ist auf der Internetseite des Europarates abrufbar. Council of Europe: Convention on Cybercrime. CETS No. 185, abrufbar unter: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG (letzter Zugriff: 18.11.2013).

cyberspace."[26] Nicht nur bleibt der Cyberraum unbestimmt, auch die Abgrenzung von Straftatbeständen und Deliktformen bleibt aus. Es handelt sich um einen klassischen Minimalkonsens. So widmet die Europäische Union dem Thema Cybersicherheit in ihren zahlreichen offiziellen Dokumenten große Aufmerksamkeit – allerdings wenig einheitlich und im Zusammenhang mit sämtlichen Formen der Cyberkriminalität.

Diffusion einer gemeinsamen Idee zur Cybersicherheit – die strategische Ausrichtung

Nach langen Verhandlungen stellten die Kommissarinnen Catherine Ashton, Cecilia Malmström und Neelie Kroes im Februar 2013 die Europäische Cybersicherheitsstrategie vor. Diese benennt die eingangs identifizierten vier Formen der Cyberkriminalität als wichtige Herausforderungen für die Gefahrenabwehr im Cyberraum. Es wird betont, dass die Union für die Verfolgung von organisierter Kriminalität im virtuellen Raum, Cyberspionage und Cyberterrorismus gewappnet sein muss. Dafür sollen innen- wie verteidigungspolitische Instrumente eingesetzt werden.[27]

Einleitend wird in der Cybersicherheitsstrategie das wirtschaftliche Potenzial beziehungsweise die Bedeutung des Cyberraums für den Wohlstand in der Europäischen Union hervorgehoben. Es heißt: „Viele Geschäftsmodelle gehen […] von der ununterbrochenen Verfügbarkeit des Internets und einem reibungslosen Funktionieren der Informationssysteme aus."[28] Mit dieser Dimension werden vor allem der Privatsektor und die individuelle, wirtschaftliche Verletzlichkeit der Bürger angesprochen. Einerseits begründet die Europäische Kommission damit ihre Zuständigkeit und andererseits wird implizit auf die Bedeutung freiheitlicher Grundrechte – ein Fundament der europäischen Idee – verwiesen.

Im Anschluss werden fünf strategische Prioritäten formuliert: Widerstandsfähigkeit gegenüber Cyberangriffen, drastische Eindämmung der Cyberkriminalität, Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten, Entwicklung der industriellen und technischen Ressourcen für Cybersicherheit, Entwicklung einer einheitlichen Strategie für den Cyberraum auf internationaler Ebene und Förderung der Grundwerte der Europäischen Union. Streng genommen, handelt es sich bei vier der fünf Prioritäten um Bereiche, für die die Kommission formell nicht zuständig ist.

Für die kurz- wie langfristigen Maßnahmen werden daher eine Vielzahl von Akteuren einbezogen und zur Kooperation aufgefordert. Strategisch fördert – und fordert – die Europäische Union auch die Zusammenarbeit und den Informationsaustausch zwischen Akteuren der Strafverfolgung und der nachrichtendienstlichen Analyse. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (kurz: EC^3) soll die Mitgliedstaaten beispielsweise sowohl operativ als auch analytisch unterstützen.[29]

Die Cybersicherheitsstrategie führt damit in vielen Punkten zusammen, was in früheren Dokumenten schrittweise vorbereitet wurde. Hierzu zählen die Mitteilungen zur Schaffung einer Informationsgesellschaft durch Bekämpfung der Computerkriminalität von 2000, zu einer globalen Partnerschaft in der Informationsgesellschaft von 2006, zum Schutz kritischer Informationsinfrastrukturen und zur digitalen Wettbewerbsfähigkeit der Union von 2009,

26 Council of the European Union: Note from Presidency to Terrorism Working Party. Summary of the initiative on countering cyber attacks conducted by terrorists and related entities, Dok. 17675/11, hier S. 6.
27 Kommission: Cybersicherheitsstrategie der EU, 2013, S. 5.
28 Ebenda, S. 2.
29 Ebenda, S. 12.

zur digitalen Agenda für Europa oder auch zum Cloud-Computing-Potenzial von 2012.[30] Alle diese Dokumente beziehen sich in der offiziellen Sprache auf wirtschaftliche Aspekte, Wettbewerb oder die Regulierung transnationaler Infrastrukturen, sprich, auf Aspekte, die in den Zuständigkeitsbereich der Kommission fallen. Allerdings werden auch in allen Dokumenten weitergehende Maßnahmen angeregt, die insbesondere auf die Ausgestaltung der inneren Sicherheit (des Raums der Freiheit, der Sicherheit und des Rechts) und in diesem Zusammenhang die effektive Bekämpfung von Cyberkriminalität abzielen. Die Argumentation lautet: Wirtschaftliches Wachstum im virtuellen Raum ist nur möglich, wenn dieser umfassend geschützt wird. Das gemeinsame Verständnis der umfassenden Sicherheit hat sich dabei schrittweise entwickelt, von einer Konzentration auf Infrastrukturen über innere Sicherheit zu einer Verbindung mit Fragen der Außen- und Sicherheitspolitik.[31]

Auffällig ist auch, dass viele Überlegungen und vorgeschlagene Maßnahmen zur Bekämpfung der Cyberkriminalität gemeinsam mit jenen zur Abwehr des internationalen Terrorismus verortet werden. Ein einschlägiges Beispiel ist die Strategie der inneren Sicherheit vom November 2010.[32] Die Tatsache, dass gleichzeitig Vorschläge gegen Cyberkriminalität und internationalen Terrorismus unterbreitet werden, ist auf bestimmte Parallelen der Phänomene zurückzuführen. Dies wird auch vom Bericht über die Umsetzung der Sicherheitsstrategie von 2008 anerkannt, der die Prioritätenliste der Europäischen Sicherheitsstrategie von 2003[33] unter anderem um Cyberkriminalität erweitert und explizit auf die Bedeutung umfassender Sicherheitskonzepte für beide Bereiche verweist.[34] Man kann also sagen, dass die für den internationalen Terrorismus entwickelten und mittlerweile konsentierten Lösungsansätze als Folien für Cyberkriminalität adaptiert werden: Ist von einem umfassenden Sicherheitskonzept die Rede, sollen interne und externe Instrumente, operative und präventiv ermittelnde Kompetenzen miteinander verbunden werden. Konkret meint das etwa eine Zusammenarbeit von Europol und dem Intelligence Analysis Centre (IntCen), wie in einem Bericht vom Oktober 2012 über die Verbesserung der Terrorismusbekämpfung gefordert.[35] Europol, als europäische Polizeibehörde, ist hauptsächlich für die Koordinierung von (operativer) Strafverfolgung im Bereich der inneren Sicherheit zuständig. Das Intelligence Analysis Centre unterstützt primär den Austausch und die Analyse von Geheimdienstinformationen der äußeren Sicherheit. Beide Institutionen sollen ebenfalls im Bereich der Cy-

30 Europäische Kommission: Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, KOM (2000) 890; Auf dem Wege zu einer globalen Partnerschaft in der Informationsgesellschaft: Folgemaßnahmen nach der Tunis-Phase des Weltgipfels über die Informationsgesellschaft (WSIS), KOM (2006) 181; Mitteilung über den Schutz kritischer Informationsinfrastrukturen. „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität", KOM (2009) 149; Bericht über die digitale Wettbewerbsfähigkeit Europas. Hauptergebnisse der i2010-Strategie 2005-2009, KOM (2009) 390; Die digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa, KOM (2012) 784; Freisetzung des Cloud-Computing-Potenzials in Europa, KOM (2012) 529.

31 Diese Herangehensweise ist in Teilen dem US-amerikanischen Vorgehen geschuldet, das in den Anfängen ebenfalls auf strafverfolgende Maßnahmen setzte und zunehmend die Kompetenzen der Nachrichtendienste mit einbezieht. Vergleiche: Holly Porteous: Cybersecurity and Intelligence: The U.S. Approach, Ottawa: Library of Parliament: Background Paper, 2011, S. 2-3.

32 Europäische Kommission: EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa, KOM (2010) 673, S. 2.

33 Rat der EU: Ein sicheres Europa in einer besseren Welt. Europäische Sicherheitsstrategie, Dok. 15895/03.

34 Europäische Kommission: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie. Sicherheit schaffen in einer Welt im Wandel, Dok. S407/08.

35 Rat der EU: Bericht zur Implementierung der Ratsschlussfolgerungen über die Verbesserung der Verknüpfung interner und externer Aspekte von Terrorismusbekämpfung, Dok. 14819/1/12, Punkt 17.

bersicherheit zusammenarbeiten.[36] Die Erfahrungen aus der Terrorismusbekämpfung gehen also in die Logik der Strategien zur Cybersicherheit über.

Bewertungen Europols nehmen ohnehin wesentlichen Einfluss auf die strategische Ausrichtung und die Politikformulierung der Europäischen Union. An einer Stelle heißt es zum Beispiel, dass Cyberkriminalität „ein hohes Maß an nachrichtendienstlicher Koordinierung und Analyse im Rahmen der Zusammenarbeit bei der Strafverfolgung erfordert."[37] Laut des Europol Terrorism and Situation Trend Report von 2012 steigt die Gefahr von ideologisch-motivierten technologischen Angriffen (beispielsweise auf kritische Infrastrukturen) unter anderem deshalb an, weil Terroristen mittlerweile hauptsächlich über das Internet kommunizieren.[38] Des Weiteren wird in der Untersuchung von organisierter Kriminalität im Cyberraum die eigentliche Motivation der Täter in der Regel erst im Verlauf deutlich. Ob die Täter Daten zu ihrem wirtschaftlichen Vorteil oder aber doch aus politischen oder ideologischen Gründen ausspähen, erklärt sich nicht allein durch ihr gewähltes Ziel und die angewandten Methoden. Der Trend Report von 2013 bestätigt dies erneut.[39] Im letzten Europol-Analysebericht von 2013 gehört Cyberkriminalität deshalb klar zu den sieben Schlüsselgefahren, denen prioritär operativ entgegen getreten werden soll.[40]

Eine solche gemeinschaftliche und umfassende Herangehensweise wird demnach von einer Vielzahl europäischer Akteure angeregt. Punktuell wird die Europäische Union auch im Rahmen rechtlicher Regulierung aktiv und fördert das gemeinsame Verständnis eines umfassenden Sicherheitskonzepts durch gemeinsame Einrichtungen und gezielte operative Erfolge.

Punktuelle vertikale Steuerung durch rechtliche Angleichung

Die Europäische Cybersicherheitsstrategie beinhaltet auch Vorschläge auf rechtlicher Ebene. So ist ihr ein Richtlinienvorschlag zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit angehängt.[41] Dies ist die dritte Richtlinie, die die strategische Ausrichtung von Cybersicherheit in rechtlicher Hinsicht flankiert. Die beiden anderen beschäftigen sich mit Angriffen auf Informationssysteme und der Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern und Kinderpornografie.[42] Die rechtliche Regulierung dient der Angleichung von Tatbeständen, strafverfolgenden Maßnahmen und der Verbesserung grenzüberschreitender Ermittlungen in den Mitgliedstaaten. Alle drei Richtlinien basieren auf konkreten Erfolgen Europols, die verdeutlichen, dass einzelstaatliche Aktivitäten in diesem Feld nicht ausreichen. Eine gemeinsame Steuerung durch

36 Rat der EU: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie, 2008, Punkt 8; ähnlich der Europäische Koordinator für Terrorismusbekämpfung: Rat der EU: EU Counter-Terrorism Strategy – Discussion paper, Dok. 9990/12, S. 4.

37 Mit Verweis auf Europol Rat der EU: Entwurf von Schlussfolgerungen zur Errichtung eines EC^3, 2012, S. 4.

38 Europol: TE-SAT 2012. EU Terrorism Situation and Trend Report, 2012, S. 6 und 12.

39 Ebenda, S. 12.

40 Europol: SOCTA 2013. EU Serious and Organised Crime Threat Assessment, Den Haag 2013, hier S. 39.

41 Kommission: Cybersicherheitsstrategie der EU, 2013, S. 8.

42 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, in: Amtsblatt der EU, Nr. L 69 vom 16. März 2005, S. 67-71; Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, in: Amtsblatt der EU, Nr. L 335 vom 17. Dezember 2011, S. 1-14. Neue Fassung: Europäische Kommission: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517.

die Europäische Union ist für ein effektives Handeln und eine erfolgreiche Bekämpfung von Cyberkriminalität notwendig und wird gezielt, zunächst in begrenzten Fällen, eingesetzt.

Vor allem die Maßnahmen auf institutioneller Ebene unterstützen die Diffusion gemeinsamer Ideen und die zunehmende Bereitschaft zu gemeinsamer rechtlicher Regulierung. Die jüngste dieser Maßnahmen ist die Einrichtung des EC^3, welches konkret zur gemeinsamen Steuerung von Cybersicherheit in der Union beitragen soll.

Institutionalisierung von Regeln und Prozeduren durch gemeinsame Einrichtungen

Das EC^3 nahm seine Arbeit am 1. Januar 2013 auf dem Gelände von Europol in Den Haag auf. Seine volle Funktionsfähigkeit soll es binnen zwei Jahren erreichen. Europol ist bereits seit mehreren Jahren mit der Verfolgung von Cyberkriminalität betraut. So wurde 2002 eigens eine Arbeitseinheit eingerichtet, das sogenannte Cyber Crime Centre. Die dort beschäftigten Experten sind zum Jahresbeginn in das EC^3 versetzt worden. Zuvor waren sie bereits an einer Reihe von Operationen beteiligt, mit deren Hilfe unter anderem Erfolge im Kampf gegen Kinderpornografie im Internet erzielt werden konnten. Im Zuge der Operation Rescue konnte beispielsweise im Bereich des Kindesmissbrauchs ein weltweit agierendes Netzwerk aufgedeckt werden, die Ermittlungen laufen seit 2011 und dauern weiterhin an. Bisher gab es 250 Festnahmen, womit es sich um eine der größten Operationen dieser Art handelt. An den Ermittlungen waren 14 Länder beteiligt. Bei der Operation Icarus, die ähnlich ausgestaltet war und ebenfalls auf die Aufklärung von sexueller Ausbeutung von Kindern zielte, waren sogar 23 Staaten involviert.[43]

Weitere Operationen im Bereich der Cyberkriminalität, die von Europol geleitet oder unterstützt wurden, sind die Operationen Crossbill und Mariposa II. Bei Crossbill wurde gegen eine Gruppierung ermittelt, die unter dem Verdacht stand, Schadsoftware zu verteilen, Bankdaten auszuspähen und mit den gestohlenen Bankdaten Geldwäsche zu betreiben. Mariposa II zielte auf sogenannte Butterfly-Bots. Solche Botnetze werden verstärkt für Finanzbetrugsdelikte genutzt. Im Kampf gegen die sich ausweitende Botinfrastruktur wurde bei Europol eine neue operative Arbeitsgruppe eingerichtet, die die Koordinierung und den Austausch von Informationen zwischen den beteiligten Staaten leitet.

Darüber hinaus existiert innerhalb Europols eine Taskforce für Cyberkriminalität in Europa, in welcher Experten aus den Mitgliedstaaten, der Kommission und Eurojust zusammenkommen, um die strategischen Vorgaben des vom Rat eingesetzten Ständigen Ausschusses für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) in operative Tätigkeiten umzuwandeln. Europol hat seit seinem Bestehen, auch im Zusammenhang mit seinen operativen Erfolgen, eine Reihe von Mandatsanpassungen durchlaufen. Zuletzt wurde es mit Wirkung zum 1. Januar 2010 in eine Europäische Agentur umgewandelt und bekam neue Kompetenzen sowohl im operativen als auch administrativen Bereich.[44] Weitere Änderungen werden im Zuge der Einrichtung des EC^3 diskutiert.[45] Das heißt, die gemeinsamen Erfahrungen und Erfolge schaffen Vertrauen und damit einhergehende Sozialisierungseffekte erlauben weitere Mandatsanpassungen.

43 Hier wie für die folgenden Ausführungen zu Europol: Europol-Jahresbericht 2011. Allgemeiner Bericht über die Tätigkeiten von Europol, Den Haag, 7.5.2012.

44 Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), in: Amtsblatt der EU, Nr. L 121 vom 15. Mai 2009, S. 37-66 (im Folgenden: Europol-Entscheidung).

45 Vergleiche Emma Disley/Barrie Irving/William Hughes/Bhanu Patruni: Technical Report. Evaluation of the Implementation of the Europol Council Decision and Europol's activities, Rand Europe 2012, S. 65 und 70.

Institutionell, finanziell und rechtlich ist das EC^3 im Rechtsrahmen von Europol verankert. Allerdings soll es ab 2014 über eine eigene Budgetlinie verfügen und nicht mehr aus dem Haushalt von Europol schöpfen. In erster Linie soll das EC^3 Cyberstraftaten aufklären und bekämpfen, die entweder auf hohe illegale Erträge zielen (zum Beispiel E-Banking, Internetbetrug), schwerwiegende Folgen für die Opfer nach sich ziehen (unter anderem Kinderpornografie) oder auf die Beeinträchtigung von kritischen Infrastrukturen und Informationssystemen abstellen (inklusive gezielter Cyberangriffe). Aus definitorischer Sicht beinhaltet der Arbeitsauftrag damit letztlich alle Formen der Cyberkriminalität.

Ausgestattet mit modernster Technik, hochqualifiziertem und spezialisiertem Personal soll sich das EC^3 als Fusionszentrum etablieren. Als Fusionszentrum führt es Daten und Informationen aus unterschiedlichen Einrichtungen und Bereichen zusammen. Ohnehin sind Informationen die wesentliche Ressource in der Arbeit einer Einrichtung wie dem EC^3. Diese werden dem Zentrum von einer Vielzahl von Akteuren – strafverfolgend wie nachrichtendienstlich – zugespielt. Es bestehen Kooperationsabkommen mit allen 28 Mitgliedstaaten, weiteren Staaten wie Norwegen, Australien oder Kolumbien sowie Einrichtungen wie dem US-amerikanischen FBI[46] und dem britischen Secret Service.[47]

Es verarbeitet jedoch nicht nur Informationen, sondern begleitet auch polizeilich relevante Maßnahmen.[48] Für diesen Teil seiner Aufgaben ist das EC^3 im Bereich der inneren Sicherheit und strafverfolgend tätig.

Das Zentrum unterteilt sich in verschiedene Teams, die jeweils eigene Bereiche abdecken. Bei der nachrichtendienstlichen Analyse arbeiten Experten, die eine ‚Helikopter-Perspektive' einnehmen und neue Entwicklungen und Trends verfolgen. Hinzukommen Strategen, die den Cyberraum horizontal scannen und Informationen auswerten. Sie sind im Bereich der äußeren Sicherheit aktiv. Zudem gibt es Ausbilder, die sich auf Trainings mit öffentlichen, privaten und akademischen Partnern konzentrieren. Sie sollen in technischer und fachlicher Hinsicht die Entwicklung und Forschung begleiten.

Das EC^3 soll den Einsatz grenzüberschreitender, operativer Untersuchungen im Cyberraum künftig intensivieren. Da es jedoch an den Rechtsrahmen von Europol gebunden ist, bleibt offen, inwieweit das EC^3 eigenständig Untersuchungen anstrengen kann und ob rechtlicher Rahmen und Arbeitsauftrag miteinander vereinbar sind. Europol ist nämlich laut Mandat nur auf Anfrage hin, nicht aber eigeninitiativ, tätig.[49] Anfragen an das EC^3 dürfen von Ermittlern, Staatsanwälten, Richtern sowie in Verbindung mit technischen und forensischen Aspekten seitens des Privatsektors gestellt werden. Das bedeutet, das EC^3 bezieht in seine Arbeit den Privatsektor gleichermaßen mit ein. Dies hat laut Kommission zwei Funktionen. Zum einen soll das Vertrauen in eine umfassende Herangehensweise an Sicherheitsbedrohungen im Cyberraum gestärkt, zum anderen die Entwicklung gemeinsamer Standards zur Berichterstattung oder Meldung von Cyberkriminalität erleichtert werden.[50] Werden solche Standards harmonisiert, können nationale Strafverfolgungsbehörden vergleichbare Delikte in anderen Ländern besser aufklären.

46 Federal Bureau of Investigation.

47 Europol: Europol-Jahresbericht 2011, 2012, S. 83; EurActiv: Cybercrime centre Chief: ‚We will focus on criminal groups or networks who steal your money', Interview mit Troels Ørting, 11.1.2013, abrufbar unter: http://www.euractiv.com/infosociety/chief-cyber-defender-swarmers-be-interview-516969 (letzter Zugriff: 18.11.2013).

48 Europäische Kommission: FAQ: The European Cybercrime Centre EC3, MEMO/13/06.

49 Art. 7 Europol-Entscheidung.

50 Europäische Kommission: Kriminalitätsbekämpfung im digitalen Zeitalter, 2012, S. 9.

Interessanter Weise erlaubt das Europol-Mandat einen Informationstransfer mit dem Privatsektor nur unter genau begrenzten Vorgaben und in Einzelfällen, etwa wenn diesbezüglich Abkommen mit internationalen Organisationen geschlossen werden.[51] Das von der Kommission erarbeitete Tätigkeitsprofil des EC^3 suggeriert nun, dass der Austausch mit privaten Partnern ausgebaut und über das bisherige Mandat hinaus gehen soll. Hier könnte zum Beispiel auch die Richtlinie Anwendung finden, welche in der Cybersicherheitsstrategie vorgeschlagen wird. Diese zielt auf den Ausbau von Programmen, die eine technische Verbindung des EC^3 mit etlichen Unternehmen der Informationsbranche (zum Beispiel Microsoft, Google, Symantec, McAfee, VISA-Master Card) ermöglichen.

Wie in der Kommissionsmitteilung zur Kriminalitätsbekämpfung im digitalen Zeitalter, den Ratsschlussfolgerungen zur Errichtung des EC^3 und der Cybersicherheitsstrategie betont, ist das vorgestellte Aufgabenspektrum des EC^3 nicht abschließend definiert. Neue Trends und Bedürfnisse müssen im Zusammenhang mit den sich weiterentwickelnden Mustern der Cyberkriminalität verfolgt und berücksichtigt werden.[52] Technischer Fortschritt ermöglicht neue Angriffsformen. Damit werden weitere Aufgaben, Tätigkeitsfelder und eventuelle Mandatsanpassungen des EC^3 im Zusammenhang mit dem Sammelbegriff der Cyberkriminalität bereits als gemeinsame Idee in den Diskurs eingebracht.

Derzeit zielt das Aufgabenspektrum auf die Verfolgung von Internetbetrug und Kindesmissbrauch, die Sicherung kritischer Infrastrukturen und die Entwicklung gemeinsamer Standards. Somit werden zwar primär in diesen Bereichen Daten ausgetauscht, allerdings handelt es sich nicht um irgendwelche Informationen, sondern um solche mit interner wie externer, strafverfolgender wie nachrichtendienstlicher Dimension.

Ebenfalls im weiten Feld der Cybersicherheit aktiv ist ENISA. Die Agentur soll dazu beitragen, europaweit eine hochgradige Netz- und Informationssicherheit zu gewährleisten. Hierfür stellt sie den Mitgliedstaaten sowie den Institutionen der Europäischen Union die notwendige Expertise zur Verfügung und dient als Sammel- und Kontaktstelle für den Austausch von Erfahrungen. Sie unterstützt Kommission und Mitgliedstaaten dabei, Probleme in der Netz- und Informationssicherheit zu erkennen und zu lösen. Ihre Hauptaufgabe liegt in der Prävention von Netzangriffen.[53]

Unter der Federführung von ENISA fanden bereits zwei europaweite Cyberabwehrübungen statt. Die erste in 2010 und die zweite in 2012. An „Cyber Europe 2012“, einer Übung zur Verbesserung der Robustheit von kritischen Infrastrukturen insbesondere im Informationsbereich, nahmen 29 Mitgliedstaaten der Europäischen Union sowie der Europäischen Freihandelszone teil. Aufgrund der Erfahrungen mit der ersten Cyberabwehrübung wurden diesmal auch Vertreter des Privatsektors hinzugezogen. Die Simulation konzentrierte sich auf sogenannte Distributed Denial of Service-Angriffe (Überlastung) auf öffentliche Dienste. Solche Angriffe können beispielsweise Regierungsseiten außer Gefecht setzen oder Informationsdienste stören, indem die Angreifer gezielt oder über Botnetze eine derart hohe Anzahl an Anfragen oder Seitenaufrufen senden, dass der Dienst überlastet und die Seite nicht erreichbar ist. Prominente Ziele in der jüngeren Vergangenheit waren unter anderem Amazon

51 Art. 23 und 25 Europol-Entscheidung.

52 Europäische Kommission: Kriminalitätsbekämpfung im digitalen Zeitalter, 2012, S. 4, Rat der EU: Entwurf von Schlussfolgerungen zur Errichtung eines EC^3, 2012, S. 5; Europäische Kommission: Cybersicherheitsstrategie der EU, 2013, S. 17.

53 ENISA: Securing Europe’s Information Society. General Report 2011, Heraklion 2012, S. 8.

oder die Stadt Frankfurt im Zuge der Blockupy-Proteste.[54] Im Nachgang konnten alle Teilnehmer Einschätzungen und Empfehlungen abgeben, wie die Zusammenarbeit weiter ausgebaut und verbessert werden kann.[55] Weitere Übungen zur Stärkung der operativen Fähigkeiten – oder anders ausgedrückt zur Förderung von Lern- und Sozialisierungsprozessen – sind vorgesehen.[56] Eine Überarbeitung und Neuausrichtung des ENISA-Mandats, inklusive einer Erhöhung der finanziellen und personellen Ressourcen, wird derzeit ebenfalls angestrebt.[57]

Die Maßnahmen zur Bekämpfung der Cyberkriminalität auf institutioneller Ebene unterstützen nicht nur die Koordinierungs- und Sozialisierungsprozesse, die für die Diffusion gemeinsamer Ideen entscheidend sind. Sie führen auch zusammen, was auf strategischer und rechtlicher Ebene initiiert wird. Im politischen Diskurs werden umfassende Sicherheitskonzepte als essenziell identifiziert. In Einrichtungen wie ENISA oder dem EC^3 werden Kooperationen und Abstimmungsmechanismen institutionalisiert.

Rückwirkungen der europäischen Maßnahmen auf die Bundesrepublik Deutschland

Auch die Bundesrepublik Deutschland richtet ihre Sicherheitspolitik zunehmend anhand der Idee eines umfassenden Sicherheitsverständnisses aus. Allerdings sind seiner Umsetzung in Deutschland gewisse strukturelle Grenzen gesetzt. Aus Gründen der Rechtssicherheit soll die Arbeit von Polizei und Nachrichtendiensten in Deutschland organisatorisch, personell und informationell getrennt bleiben.[58] Ein solches Gebot gibt es nicht in allen EU-Ländern. In der Bundesrepublik ist das Trennungsgebot historisch gewachsen. Es resultiert aus den einschneidenden Erfahrungen mit der Geheimen Staatspolizei zu Zeiten des Nationalsozialismus. Diese instrumentalisierte ihr nachrichtendienstlich gewonnenes Wissen, indem sie politisch motivierte Strafmaßnahmen durchsetzte. Die Aufgaben von Strafverfolgungsbehörden und Polizei sind in Deutschland seither auf die konkrete Gefahrenabwehr beschränkt, die Aufgaben der Nachrichtendienste auf Aufklärung und Bedrohungsanalysen. Das bedeutet, die Strafverfolgungsbehörden dürfen erst mit dem Vorliegen eines tatsächlichen Verdachts tätig werden. Während die Nachrichtendienste nicht polizeilich eingreifen dürfen, sondern nur Bedrohungen anzeigen. Der Zusammenarbeit sind somit rechtlich Grenzen gesetzt. Ein Austausch von Informationen ist – zumindest in der Bundesrepublik – nur zulässig, wenn er anlassbezogen und im Einzelfall erfolgt.

Seit den Anschlägen des 11. September 2001 hat der Druck, sich zu koordinieren und international auszutauschen, enorm zugenommen. Die strategische Ausrichtung der Europäischen Union im Feld der Cybersicherheit, die sich verstärkt für eine Verbindung von internen und externen Instrumenten der Sicherheit sowie eine Zusammenführung operativer

54 Eine Auflistung möglicher DDoS-Angriffe sowie von Gegenmaßnahmen findet sich zum Beispiel bei: Christoph Puppe/Jörn Maier: Von allen Seiten, in: iX Magazin für professionelle Informationstechnik 4/2005, S. 107-112.

55 ENISA: Cyber Europe 2012. Wichtigste Erkenntnisse und Empfehlungen, Heraklion 2012.

56 Europäische Kommission: Cybersicherheitsstrategie der EU, 2013, S. 7-8.

57 Europäisches Parlament: Legislative Entschließung und Standpunkt des Europäischen Parlaments zur Verordnung über die Europäische Agentur für Netz- und Informationssicherheit, P7_TA(2013)0103. Zunächst gilt das Mandat bis September 2013. Vgl. Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, in: Amtsblatt der EU, Nr. L 165 vom 24. Juni 2011, S. 3-4.

58 Jens Singer: Das Trennungsgebot – Teil 1. Politisches Schlagwort oder verfassungsrechtliche Vorgabe?, in: Die Kriminalpolizei, Berlin 2006, S. 112-117.

und nachrichtendienstlicher Informationen einsetzt, hat auch Folgen für die deutsche Gesetzgebung sowie die Neuaufstellung nationaler Sicherheitsbehörden.[59]

Der Bedarf an Cybersicherheit ist nach Angaben der nationalen Behörden enorm hoch. Monatlich werden bis zu 30.000 Zugriffsversuche auf schädliche Webseiten aus dem Regierungsnetz registriert. Pro Minute werden allein in Deutschland statistisch zwei Identitäten mithilfe des Internets gestohlen.[60] Die offiziellen Dokumente veranschaulichen die Relevanz von Cybersicherheit auch anhand von prominenten Beispielen wie Stuxnet. Bei Stuxnet handelte es sich um einen Trojaner, mit dessen Hilfe das iranische Nuklearprogramm infiltriert und kurzfristig ferngesteuert wurde. Komplexe Schadprogramme dieser Art sind auf Eingriffe in Prozesssteuerungen und die Störung kritischer Infrastrukturen angelegt. Das Fazit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Fall von Stuxnet lautet: Hierdurch „wird deutlich, dass die gesamte Sicherheitskonzeption von Systemen zur Prozesssteuerung dringlich zu überdenken, und, wo notwendig, der aktuellen Bedrohungslage anzupassen ist.“[61] Für mögliche Lösungsansätze und neue Sicherheitskonzepte schaut man zu den europäischen Partnern sowie insbesondere zu den gemeinsamen Einrichtungen, die einen breiteren, horizontalen Einblick haben. Weitere Formen von Cyberangriffen, für welche sich die Bundesrepublik wappnen und zu deren Bekämpfung ein Nationales Cyber-Abwehrzentrum beitragen soll, sind Identitätsdiebstahl, Hacking, Botnetze, Spam, Distributed Denial of Service-Angriffe und Internet-Strukturangriffe.[62] Die Erfolge von Europol und die Cyberabwehrübungen von ENISA fördern gerade in diesen Bereichen eine europaweite Angleichung und Kooperation, indem einerseits ‚best practices‘ identifiziert und anderseits Steuerungsfunktionen institutionalisiert werden. Regeln und Idee werden transnational auf europäischer Ebene entwickelt und dann in die nationale Logik der Politikgestaltung überführt.

Der Rahmen für Cybersicherheit ist auf nationaler Ebene daher genauso weit gespannt wie in der Europäischen Union und umfasst folglich mehrere Politikbereiche. Ein Teil dieser Entwicklungen ist direkt auf die Verpflichtungen aus dem Primärrecht und der entsprechenden Sekundärrechtslage zurückzuführen.[63] Mit den Reformen wurde Cybersicherheit zu einer sicherheitspolitischen Priorität der Europäischen Union. Auf strategischer Ebene hat sich die Bundesrepublik Deutschland 2011 dazu in ihrer Cybersicherheitsstrategie positioniert. [64] Die Notwendigkeit, nationale Cybersicherheitsstrategien zu entwickeln, kann auf die Strategie der inneren Sicherheit der Europäischen Union aus dem Jahr 2010 zurückgeführt werden – zuvor verfügten lediglich Estland, die Slowakei und Großbritannien über entsprechende Strategien. Darüber hinaus ist ENISA beauftragt worden, einen ‚Good Practice Guide‘ zu entwickeln, um den Mitgliedstaaten die Verabschiedung und Überprüfung

59 Vergleiche: Mariaelisa Epifanio: Legislative response to international terrorism, in: Journal of Peace Research 3/2011, S. 399-411; Franco Algieri: Deutschen Außen- und Sicherheitspolitik im europäischen Kontext: Zur Parallelität von Kontinuität und Wandel, in: Thomas Jäger/Alexander Höse/Kai Oppermann (Hrsg.): Deutsche Außenpolitik, Wiesbaden 2007, S. 106-122; Thomas Risse: Kontinuität durch Wandel: Eine „neue“ deutsche Außenpolitik?, in: Aus Politik und Zeitgeschichte 11/2004, S. 24-31.

60 Hartmut Isselhorst, BSI: Präsentation des Nationalen Cyber-Abwehrzentrums, Bonn 16. Juni 2011.

61 Bundesamt für Sicherheit in der Informationstechnologie: Die Lage der IT-Sicherheit in Deutschland 2011, Bonn 2011, S. 29.

62 Isselhorst: Präsentation des Nationalen Cyber-Abwehrzentrums, 2011.

63 Siehe hierzu die Debatte, wonach Solidaritäts- und die Beistandsklausel auch auf Cyberangriffe angewendet werden sollen: Europäisches Parlament: Entschließung zu Cyber-Sicherheit und Verteidigung, 2012.

64 Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, Berlin 2011.

ihrer Cybersicherheitsstrategien zu erleichtern.[65] Auf diese Weise werden horizontale Impulse gegeben, die der Entwicklung gemeinsamer Vorstellungen und Grundlagen dienen.

In der deutschen Cybersicherheitsstrategie wird explizit betont, dass die Gefahren sowohl krimineller als auch terroristischer, nachrichtendienstlicher und mitunter militärischer Natur sind und daher eine Mischung aus innen- und außenpolitischen Instrumenten notwendig ist.[66] Hier lässt sich eine enge Verbindung – im Sinne einer Übernahme von Begründungsmustern und Konzepten – mit den Strategiedokumenten der Europäischen Union wahrnehmen, allen voran der Europäischen Sicherheitsstrategie von 2003 sowie dem Implementierungsbericht von 2008, die den umfassenden Sicherheitsansatz nachdrücklich prägen. Die Bundesregierung listet zehn Maßnahmen auf, die erst teilweise umgesetzt sind. Dies sind der Schutz kritischer Infrastrukturen, sichere IT-Systeme, die Stärkung der IT-Sicherheit und der öffentlichen Verwaltung, die Einrichtung des Nationalen Cyber-Abwehrzentrums sowie eines Nationalen Cyber-Sicherheitsrates, eine wirksame Kriminalitätsbekämpfung im Cyberraum, die Verbesserung der Zusammenarbeit in der Europäischen Union und der Welt diesbezüglich, die Entwicklung und der Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie, die Förderung der entsprechenden Personalentwicklung in den Bundesbehörden sowie der Aufbau eines Instrumentariums zur Abwehr von Cyberangriffen.

Auf institutioneller Ebene ist unter anderem eine Zusammenarbeit zwischen dem 2012 eingerichteten ständigen Computer Emergency Response Team (CERT) der Europäischen Union und den nationalen CERT normiert.[67] Die Aufgabe der CERT liegt in der Sammlung und Auswertung von Sicherheitslücken und neuen Angriffsmustern. Sie geben diese Informationen und Warnungen an die betroffenen Stellen sowie die Öffentlichkeit weiter. Damit dienen sie als Kontaktstellen zwischen nationalen und internationalen Partnern.

In Deutschland wurde ein CERT im BSI eingerichtet. Die Vernetzung und praktische Zusammenarbeit von deutschem und EU-CERT befindet sich jedoch noch in den Anfängen und soll schrittweise auf- und ausgebaut werden.

Darüber hinaus wurde im April 2011 das Nationale Cyber-Abwehrzentrum eröffnet, dessen Einrichtung auf den Erfahrungen mit dem Gemeinsamen Terrorabwehrzentrum aufbaut. Es hat seinen Sitz in Bonn und ist ebenfalls beim BSI angesiedelt. Allerdings ist das Nationale Cyber-Abwehrzentrum keine Behörde im engeren Sinne, weshalb sein Arbeitsauftrag nicht gesetzlich geregelt ist. Es agiert im Rahmen von Kooperationsvereinbarungen zwischen den beteiligten Einrichtungen. Dazu zählen das BSI, das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie als assoziierte Behörden der Bundesnachrichtendienst (BND), das Bundeskriminalamt (BKA) und die Bundeswehr.[68]

Das Nationale Cyber-Abwehrzentrum soll den Informationsaustausch erleichtern, Schwachstellen analysieren und Handlungsempfehlungen entwickeln. Dabei dient es der „Optimierung der operativen Zusammenarbeit".[69] Diese operative Zusammenarbeit be-

65 Vergleiche ENISA: Good Practice Guide on National Cyber Security Strategies, abrufbar unter: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss (letzter Zugriff: 23.8.2013).

66 Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, 2011, S. 3-4.

67 Zum Kontext und der Umsetzung der digitalen Agenda siehe ENISA: CERT-EU, abrufbar unter: http://www.enisa.europa.eu/activities/cert/background/inv/cert-eu (letzter Zugriff: 18.11.2013).

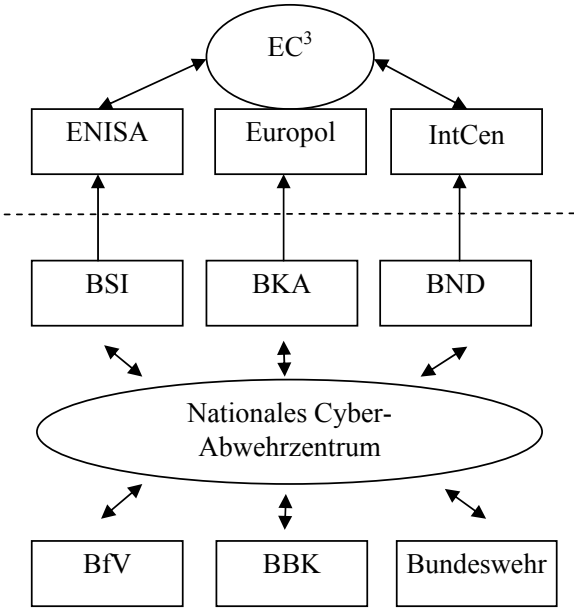
68 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau u.a. und der Fraktion Die Linke – Drucksache 17/5560 – Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Das Nationale Cyber-Abwehrzentrum, in: Bundestagsdrucksache 17/5694.

69 Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, 2011, S. 8.

schränkt sich nicht auf das nationale Hoheitsgebiet, sondern bezieht eine enge Kooperation von Strafverfolgungsbehörden weltweit ein. Die gemeinsame Prämisse bildet die virtuelle Grenzenlosigkeit des Cyberraums und damit auch der Kriminalität – eine Argumentation, die sich in so ziemlich allen Strategiedokumenten der Europäischen Kommission finden lässt.

Im neu gegründeten Nationalen Cyber-Sicherheitsrat sind das Bundeskanzleramt sowie auf Ebene der Staatssekretäre das Auswärtige Amt, das Bundesministerium des Innern, das Bundesministerium der Verteidigung, das Bundesministerium für Wirtschaft und Technologie, das Bundesministerium der Justiz, das Bundesministerium der Finanzen, das Bundesministerium für Bildung und Forschung und die Länder vertreten. Zu bestimmten Anlässen können weitere Ressorts sowie Wirtschaftsvertreter als assoziierte Mitglieder eingeladen werden. Auch Vertreter aus der Wissenschaft werden bei Bedarf konsultiert.[70] Diese Herangehensweise hat sich bei Europol bewährt und soll jetzt im EC^3 weiter vertieft werden. Der Cyber-Sicherheitsrat ist zuständig für die politisch-strategische Ebene der zu ergreifenden Maßnahmen und soll die präventiven Instrumente sowie die Politikansätze von Staat und Wirtschaft zur Cybersicherheit koordinieren.

Abbildung 1: Informationsfluss zwischen europäischen und nationalen Einrichtungen



Quelle: Eigene Darstellung.

Das neu eingerichtete EC^3 unterstützt die nationalen Bemühungen und treibt diesen Prozess der Angleichung und Abstimmung nun weiter voran. Je nach Aufgabenteilung in den Mitgliedstaaten sind nämlich unterschiedliche Behörden angehalten, die jeweils relevanten Informationen für die Arbeit des Zentrums weiterzugeben. In der Bundesrepublik Deutsch-

70 Ebenda, S. 9-10.

land umfasst dies unter anderem das Bundeskriminalamt, das BSI und den Bundesnachrichtendienst. Eine direkte Zusammenarbeit des EC^3 mit dem Nationalen Cyber-Abwehrzentrum ist interessanter Weise bislang nicht vorgesehen. Die dort gewonnenen Erkenntnisse werden über die bestehenden Kooperationsabsprachen der beteiligten Behörden mit den europäischen Institutionen weitergegeben.[71] Das bedeutet, Erkenntnisse aus dem Cyber-Abwehrzentrum werden über das BSI an ENISA, über das Bundeskriminalamt an Europol oder den Bundesnachrichtendienst an das Intelligence Analysis Centre übermittelt. Auf nationaler Ebene bleiben die Behörden und ihr Personal damit organisatorisch getrennt. Allerdings findet der Informationsaustausch beziehungsweise die Zusammenführung der Informationen im (organisatorisch nicht getrennten) EC^3 weniger in Einzelfällen als allgemein im Bereich Cyberkriminalität statt. Immerhin speisen sowohl ENISA als auch Europol und Intelligence Analysis Centre Informationen ins EC^3 ein.

Zusammenfassend ist festzuhalten, dass ein Teil der Politikgestaltungsprozesse parallel abläuft, die große Bandbreite der Impulse jedoch durch die Europäische Union definiert und zunehmend auch konsolidiert wird. Innerhalb Deutschlands lässt sich derzeit im Zusammenhang mit einem umfassenden Sicherheitskonzept und dem dazugehörigen Informationsaustausch ein Ausreizen der Grenzen des rechtlich Möglichen wahrnehmen. Gemeint sind hier in erster Linie die Kooperationsvereinbarungen, die die Grundlage für die Arbeit der gemeinsamen Abwehrzentren – Terror wie Cyber – bilden. Verstärkt durch Lernprozesse und einen weiteren Sozialisations- und Anpassungsdruck auf europäischer Ebene, der nicht selten Mandatsanpassungen/-ausweitungen gemeinsamer Einrichtungen, wie Europol und ENISA, nach sich zieht, scheint eine klare Trennung von Aufgabenbereichen immer schwieriger zu werden. Besonders kritisch ist die Zusammenführung von Informationen aus Bundesnachrichtendienst, Verfassungsschutz oder Bundeskriminalamt in einem personell und organisatorisch nicht getrennten Zentrum wie dem EC^3. Es ist nicht zu vergessen, dass das Zentrum nach Zustimmung der Mitgliedstaaten sogar an operativen, strafverfolgenden Maßnahmen direkt beteiligt ist. Dies ist im Licht des deutschen Trennungsgebots kritisch zu beurteilen.

Europäisierte Cybersicherheit: beabsichtigte Konsequenzen?

Das relativ junge Politikfeld der Cybersicherheit zeichnet sich durch eine große Dynamik aus. Innerhalb weniger Jahre sind auf europäischer wie nationaler Ebene eine Vielzahl an Maßnahmen ergriffen worden, die sich dem Thema annehmen. Dabei ist die Formulierung einer gemeinsamen Cybersicherheitspolitik noch lange nicht ausgereift. Strategiepapiere der Europäischen Union, operative Erfolge und gemeinsame Aktionen steuern den Politikgestaltungsprozess. Es dominieren umfassende Sicherheitskonzepte, die sich auf eine Verbindung von internen und externen, strafverfolgenden und nachrichtendienstlichen Instrumenten stützen.

Bestehende nationale Konzepte werden nicht zurückgebaut, beibehalten oder in ihrer funktionalen Logik transformiert – sie werden an europäische Vorgaben angepasst. Häufig dienen die mehr oder minder erprobten Lösungsansätze zur Bekämpfung des internationalen Terrorismus als Folie für den Umgang mit Cyberkriminalität auf europäischer wie nationaler Ebene. Allerdings hat auch die ‚nur' schrittweise Anpassung an das europäische Sicher-

71 Antwort der Bundesregierung auf die Kleine Anfrage, 2011, S. 7.

heitskonzept weitreichende Konsequenzen für die Bundesrepublik Deutschland, die es einzuordnen und zu begleiten gilt.

Während die Entwicklungen im Cyberraum die personelle und organisatorische Trennung von Strafverfolgungsbehörden und Nachrichtendiensten bisher mehr oder weniger unberührt lassen, werfen sie im Bereich des Datenaustausches und -abgleichs erhebliche Fragen auf. Der Datenaustausch zwischen Akteuren auf europäischer Ebene, etwa zwischen Europol und dem Intelligence Analysis Centre, erfolgt weniger punktuell und auf Einzelfälle bezogen als systematisch im Zusammenhang mit den komplexen oder umfassenden Formen der Cyberkriminalität. Die Zusammenführung von Informationen aus verschiedenen Diensten der Mitgliedstaaten resultiert aus den umfassenden Sicherheitskonzepten, weicht aber die informationelle Trennung, die im Falle Deutschlands normiert ist, klar auf.

Die Frage, ob das Trennungsgebot in dieser Hinsicht noch zeitgemäß ist, kann überspitzt auf zwei Arten beantwortet werden: Nein, da die eingeleitete Entwicklung notwendig und zielführend ist, um mit den sich ständig weiter ausdifferenzierenden Kriminalitätsformen mithalten zu können. In diesem Fall sollte die Auflösung des Trennungsgebots ehrlich diskutiert und vor allem die Debatte über ein abgestimmtes europäisches Verständnis von Cybersicherheit forciert werden.

Die andere Antwort lautet: Ja, da nur so Eingriffen in die Grundrechte vorgebeugt und entgegengewirkt werden kann – man denke speziell an die anhaltenden Enthüllungen über Prism oder die Befragung von Journalisten auf Grundlage von Sonderregelungen der britischen Anti-Terror-Gesetze. In jedem Fall müssen dann sowohl Datenschutz als auch Grenzen einer Kooperation diskutiert werden. Die Übermittlung von Daten muss an klare Bedingungen geknüpft werden und zwar nicht nur auf nationaler Ebene, sondern auch in den Mandaten der europäischen Einrichtungen.

Dies führt zu einem weiteren Aspekt, auf den sich die Europäisierung von Cybersicherheitspolitik auswirkt: die demokratische Kontrolle. So notwendig Mandatsanpassungen sein mögen, muss doch sichergestellt sein, dass eine Kompetenzausweitung immer mit der notwendigen (richterlichen wie parlamentarischen) Kontrolle einhergeht. Daher sollten Europäischem und nationalen Parlamenten auch inhaltliche Kontrollrechte zugesprochen werden. Derzeit ist das EC^3 zum Beispiel aufgrund der Rechtsanbindung an Europol nur gegenüber dem Rat der Europäischen Union rechenschaftspflichtig. Es erstattet im Rat für Justiz und Inneres Bericht. Innerhalb Deutschlands liegt die Informationshoheit somit beim Bundesministerium des Inneren. Sobald das EC^3 ab 2014 über eine eigene Budgetlinie verfügt, kann das Europäische Parlament im Rahmen der Verhandlungen über Personalstärke und operative Mittel formal eine gewisse Kontrolle ausüben, eine inhaltliche Überprüfung findet aber nur indirekt statt, etwa über Begründungen bei Mittelanträgen. Fragen der Datensicherheit, wie das Ausmaß der Verwendung und Speicherung übermittelter und gesammelter Daten, sind so kaum transparent. Die fehlende Rechenschaftspflicht gegenüber dem Europäischen Parlament erschwert zudem die transparente Kontrolle über die Einhaltung von Grundrechten (informationelle Selbstbestimmung, Schutz der Privatsphäre) in der Arbeit des EC^3.

Auf nationaler Ebene sollten die Informationsrechte effektiv genutzt und die nationalen Dienste verpflichtet werden, ihre europäischen Aktivitäten offenzulegen. Gegebenenfalls muss die Balance zwischen Geheimnisschutz und Öffentlichkeitsprinzip neu austariert werden. Auf diese Weise könnte zum Beispiel der Deutsche Bundestag den konkreten Einfluss von Nachrichtendiensten auf strafverfolgende und polizeiliche Maßnahmen überprüfen.

Die Neugewichtung der parlamentarischen Kontrolle ist auch wichtig, um eine breitere Debatte, die sich nicht nur auf europäische Eliten oder Expertenkreise beschränkt, anzusto-

ßen. Nur so kann sinnvoll zwischen notwendigen und ausufernden Maßnahmen sowie erwünschten und unerwünschten Konsequenzen der Europäisierung unterschieden werden.