Die Verfassung des Internets

Die EU muss eine gemeinsame Strategie für Cybersicherheit erarbeiten

Annegret Bendiek und Ben Wagner | **Bevor auf globaler Ebene darüber entschieden wird, wie das Internet reguliert werden soll und welche normativen Grundlagen überhaupt gelten, müssen die Europäer eine gemeinsame Haltung entwickeln. Eine solche EU-Strategie sollte aber nicht Sicherheit gegen Freiheit oder Staat gegen Private gegeneinander ausspielen.**

Die globale Cyberpolitik befindet sich in einer entscheidenden Phase. Im Dezember 2012 werden Vertreter von über 190 Staaten in Dubai über die International Telecommunications Regulations (ITRs) verhandeln, wobei nicht nur die Regulierung, sondern auch die normativen Grundlagen des Internets der Zukunft beraten werden. Dabei stellen sich folgende Fragen: Wie viel Freiheit soll das Internet gewährleisten, welche Sicherheitsvorkehrungen muss es gegen Kriminalität und Terrorismus geben und wo sollen die Grenzen zwischen nationaler Selbstbestimmung und globalem Raum verlaufen? Wird es zukünftig überhaupt noch ein globales Internet geben oder verstärkt sich der bereits zu beobachtende Trend einer Fragmentierung des Netzes und vermehrter nationaler Kontrolle über Zugang und Inhalte?

Die EU koordiniert die nationalen Politiken ihrer 27 Mitgliedstaaten und verwaltet den größten Binnenmarkt der Welt. Entscheidungen, die in der EU getroffen werden, haben auch eine hohe Relevanz für den Rest der Welt. In der aktuellen Debatte um eine EU-Strategie zur Cybersicherheit stoßen ganz unterschiedliche Verständnisse des angemessenen Verhältnisses von Staat und Gesellschaft, von Sicherheit und Freiheit und von intergouvernemental versus parlamentarisch geprägter Politik aufeinander. Wie sie miteinander in Beziehung gesetzt werden und welche langfristigen Entscheidungen hier getroffen werden, wird die neue Ordnung des Cyberspace in den nächsten Jahren entscheidend prägen.

Freiheitsrechte und Sicherheit

Der Schutz vor Wirtschaftsspionage ist ein wichtiger Standortfaktor. Der elektronische Handel macht EU-weit 4 Prozent des Gesamthandels aus, mit stark steigender Tendenz. Eine Untersuchung von 13 hochentwickelten Staaten schätzt, dass das Internet zwi-

schen 2004 und 2009 zu 11 Prozent des BIP-Wachstums beigetragen hat.[1] Schätzungen zufolge könnten die Verbraucher insgesamt über 200 Milliarden Euro sparen, würde der elektronische Handel stärker genutzt. Dies setzt aber hohes Vertrauen in die Netzsicherheit voraus.

Den Verteidigungspolitischen Leitlinien der Bundesregierung vom Mai 2011 zufolge steht die Cybersicherheit bereits an zweiter Stelle der Sicherheitsbedrohungen. Bis Juni 2012 haben zehn EU-Staaten nationale Cybersicherheitsstrategien verabschiedet.[2] In über 30 Ländern gibt es heute Cybereinheiten im Rahmen der Streitkräfte. Cyberangriffe sind faktisch zum strategischen Kalkül einer neuen computergestützten Auseinandersetzung sowohl zwischen nichtstaatlichen und staatlichen Akteuren sowie zwischen Staaten geworden. Eindrückliche Beispiele für dieses Verständnis sind die seit 2010 zwischen den EU-Staaten und den USA regelmäßig stattfindenden Übungen zur Abwehr von Cyberangriffen. Dieser Trend setzt sich in der im November 2010 gegründeten EU-USA-Arbeitsgruppe zur Cybersicherheit fort.

Das Ziel: parlamentarische Kontrolle und rechtlich verbindliche Regelungen in der Cyberpolitik

Sicherheitsprobleme sind zweifelsohne eine wichtige Herausforderung für die Regulierung des Internets. Eine übermäßige Betonung des Sicherheitsaspekts und eine Vernachlässigung der Idee des Cyberspace als eines globalen öffentlichen Gutes können jedoch zu einer Gefahr für die Grundrechte und damit die Demokratie zu werden. Sicherheit sollte nicht als ein Gegenstand der Politik verstanden werden, der oberhalb der Demokratie steht. Wie und im Rahmen welcher Maßnahmen so genannte „kritische Infrastrukturen“ (Energie, Verkehr, Gesundheit) geschützt werden und wie bei diesem Schutz mit den privaten Informationen umgegangen wird (Stichwort: Vorratsdatenspeicherung), sollte nicht nur in Expertengremien beraten und entschieden werden. Das gehört ins Parlament.

Private Selbstregulierung ist ein Instrument. Wenn allerdings Fragen der informationellen Selbstbestimmung, der Freiheit und der demokratischen Grundrechte tangiert werden, dann kann eine demokratieverträgliche Lösung nur eine rechtsstaatliche und damit parlamentarisch geprägte Lösung sein. Doch Forderungen nach parlamentarischer Kontrolle und rechtlich verbindlichen Regulierungen in der Cyberpolitik spiegeln sich derzeit weder auf der internationalen noch der europäischen Ebene wider.

Das internationale Umfeld

In der aktuellen Debatte stehen sich zwei grundlegende und gleichermaßen unbefriedigende Positionen gegenüber. Auf der einen Seite wurde von den Mitgliedern der Schanghai-Gruppe (China, Russland, Usbekistan und Tadschikistan) 2011 die Ver-

[1] Matthieu Pélissié du Rausas: Internet matters the net’s sweeping impact on growth, jobs, and prosperity, McKinsey Global Institute 2011.
[2] Estland, Finnland, Slowakei, Tschechische Republik, Frankreich, Deutschland, Litauen, Luxemburg, die Niederlande, Großbritannien. ENISA, Mai 2012.

abschiedung eines zwischenstaatlichen „Internationalen Verhaltenskodex für Informationssicherheit“ vorgeschlagen. Dieser sollte globale Standards für „unannehmbares staatliches Verhalten“ formulieren. Die von Aktivitäten im Internet bedrohte Souveränität von Staaten sollte gestärkt und jede Einmischung in die inneren Angelegenheiten eines Staates verboten werden. Institutionell sollten die International Telecommunication Union (ITU) gestärkt, die ITR überarbeitet und die derzeit bei dem US-Unternehmen Internet Corporation for Assigend Names und Numbers (ICANN) angesiedelte Vergabe von Internetdomains auf die ITU übertragen werden.

Den chinesisch-russischen Vorschlägen steht das von den USA und den meisten OECD-Staaten präferierte so genannte Multistakeholder-Modell gegenüber. Es läuft im Wesentlichen darauf hinaus, all jenen die Teilhabe an der Regulierung des Internets zu ermöglichen, die entweder über relevantes Expertenwissen (Unternehmen, Wissenschaft), politische Autorität (Staaten) oder über gesellschaftliche Legitimation (Zivilgesellschaft) verfügen. Es ist eine sehr viel pluralistischere Form der Regulierung. So setzt die im Mai 2011 von US-Präsident Barack Obama verkündete International Strategy for Cyberspace auf transnationale Dialoge über Verhaltensnormen und vertrauensbildende Maßnahmen unter Einbindung nichtstaatlicher Akteure. Einen internationalen Vertrag lehnen die USA mit dem Argument ab, dass dieser zu starr, zu wenig verifizierbar und zu sehr auf staatliches Handeln ausgerichtet sei.

Doch keine dieser beiden Positionen kann überzeugen: Während der russisch-chinesische Vorschlag einseitig auf die Ausdehnung staatlicher Kontrollmacht abzielt, bringt das Multistakeholder-Modell fast ausschließlich die Interessen der OECD-Staaten,

insbesondere der Vereinigten Staaten, und global agierender Unternehmen zum Ausdruck. Darüber hinaus weisen beide Modelle erhebliche demokratische Legitimationsdefizite auf.

Prioritäten für Europa

Wesentliche Impulse für nationale Cybersicherheitsstrategien in Europa sind aus den USA gekommen, aus dem Land, das sich energisch für die Kriegsführung mit den Mitteln des Internets rüstet. Nach den Cyberangriffen auf Estland 2007 hat die NATO 2008 in Tallinn ein Exzellenzzentrum zur Cyberverteidigung geschaffen. Als Verteidigungsbündnis bleibt ihr Auftrag auf die militärischen Aspekte von Cybersicherheit begrenzt. Die EU wird diesen technologischen Vorsprung im militärischen Bereich absehbar nicht einholen können. Deshalb sind folgende Punkte wichtig:

1. Priorität für die EU sollte es sein, die bestehende Architektur des Internets mit seinen offenen Standards und der dezentralen Verwaltung beizubehalten. Der Multistakeholder-Ansatz und multilaterales Handeln wären in ein konstruktives Miteinander und weniger Gegeneinander zu setzen. Hierbei ist die gleichberechtigte Einbindung des „globalen Südens“ und der BRIC-Staaten von höchster Priorität.
2. Europäische Politik sollte auf die vollständige Implementierung des Europarat-Übereinkommens gerichtet sein. Dieses so genannte Budapest-Übereinkommen aus dem Jahr 2001 enthält bereits gemeinsame Definitionen der verschiedenen Arten von Internetkriminalität und bildet eine Grundlage für eine engere Zusammenarbeit zwischen den Mitgliedstaaten des Europarats sowie einigen außereuropäischen Staaten wie den USA, Japan und Kanada. Private Akteure und andere nichteuropäische Staaten sollten in die Formulierung neuer Regeln eingebunden werden.
3. Das bestehende Multistakeholder-Modell wäre zu demokratisieren und multilateral so weiterzuentwickeln, dass die Expertise privater Unternehmen eingebunden wird und dass diese gleichzeitig auf die Einhaltung globaler Standards in den Bereichen Sicherheit, informationelle Selbstbestimmung und Datenschutz festgelegt werden können.
4. Die EU sollte sich für die Aktualisierung des General Comments zu Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte durch den UN-Menschenrechtsausschuss einsetzen, in dem das Recht auf Privatsphäre verankert ist. Eine solche rechtsverbindliche Interpretation des internationalen Menschenrechtsschutzes der Privatsphäre hat zuletzt 1988 stattgefunden und bedarf dringend einer Novellierung.
5. In Bezug auf die Verhaltensnormen im Cyberspace sollte ein Instrument zur Förderung rechtlicher Verbindlichkeit greifen. Werden beispielsweise Verstöße über den UN-Menschenrechtsausschuss bekannt und dokumentiert, könnten Sanktionen ähnlich dem Prinzip zur Einsetzung des Internationalen Strafgerichtshofs verhängt werden.

Insgesamt geht es darum, eine transnationale Sicherheits- und Rechtspartnerschaft zu etablieren, die sowohl Staaten als auch Unternehmen umfasst und die neben der Sicherheit den Werten der Demokratie und der Rechtsstaatlichkeit verpflichtet ist. Es wäre damit eine europäische Strategie, die nicht Sicherheit gegen Freiheit oder Staat gegen Private auszuspielen versucht. Eine zukünftige EU-Strategie sollte als Scharnier zwischen der internationalen Ebene und den Mitgliedstaaten fungieren sowie nach innen in die Mitgliedstaaten hineinwirken.

Die EU auf dem Pfad der Sicherheit

Mit dem Implementierungsbericht zur Europäischen Sicherheitsstrategie hat der Europäische Rat die EU im Dezember 2008 ausdrücklich dazu aufgefordert, die Möglichkeiten für ein umfassendes Konzept der EU für die Cyberpolitik zu erarbeiten. Hierbei wären die Aspekte der Sicherheit gegen die Rechte des Einzelnen auf Freiheit und Selbstbestimmung abzuwägen. Eine überzeugende Antwort für diese Aufgabe bleiben die bisher vorgelegten Vorschläge allerdings schuldig. Der eingeschlagene EU-Pfad ist eindeutig zugunsten der Sicherheitsagenda ausgerichtet.

Der Europäische Rat hat im Dezember 2009 das so genannte Stockholmer Programm verabschiedet. Das „Mehrjahresprogramm für einen Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“ zielt auf „eine umfassende Unionsstrategie der inneren Sicherheit“ ab, bei der datenschutzrechtliche Fragen nur noch untergeordnete Bedeutung haben. Die Kommission reagierte auf das Stockholmer Programm nicht mit einem umfassenden Aktionsplan zur Ausdehnung von Bürgerfreiheiten und -rechten, sondern mit einer Mitteilung, in der sie schwere und organisierte Kriminalität, Cyberkriminalität, Terrorismus, Grenzsicherung und Katastrophenabwehr als akute gemeinsame Probleme benannte.

Das Thema der Sicherheit und Freiheit im Internet ist erst seit dem Arabischen Frühling in der breiteren außenpolitischen Debatte der EU angelangt. Die Diskussion über die Verantwortung von Unternehmen wie Facebook, Google und Vodafone während des Arabischen Frühlings hat den Blick dafür geschärft, dass es bei der zukünftigen Verfassung des Internets ebenfalls um die Förderung von Demokratie und den Schutz von Grundrechten auch außerhalb von Europa geht.

Bei der künftigen Verfassung des Internets geht es auch um die Förderung von Demokratie und Freiheit

In Vorbereitung auf die von der britischen Regierung initiierte Cyberkonferenz im November 2011 haben die EU-Kommissarinnen Neelie Kroes (Digitale Agenda), Cecilia Malmström (Inneres) und Catherine Ashton (Außen- und Sicherheitspolitik) im Oktober 2011 ein so genanntes „Food-for-Thought Paper“ zu Verhaltensnormen im Cyberraum entwickelt. Die hier noch recht stark betonte Rolle von demokratischen Werten hat in dem neuen Kommissionsvorschlag für eine EU-Strategie zur Cybersicherheit vom Mai 2012 einem pragmatischeren Ansatz Platz gemacht. Die Schaffung eines sicheren digitalen Umfelds für Bürger, Unternehmen und Verwaltungen sowie die

Verhinderung von Cyberkriminalität werden im Kommissionsvorschlag zur Priorität erklärt. Hierzu zählen ein schnelles Internet, interoperable Anwendungen und selbstregulierende private Konzerne.

Die jüngste Initiative fügt sich damit nahtlos in die von EU-Kommissarin Kroes betriebene „Digitale Agenda für Europa" ein. Neue Computer Emergency Response Teams (CERTs) sollen die Informationslücken zwischen dem privaten und öffentlichen Sektor schließen und den eigenen EU-CERT, als auf die EU-Ebene spezialisierte Gruppe von IT-Sicherheitsexperten, ergänzen. Zudem zielt der Kommissionsentwurf zur EU-Strategie auf eine Stärkung der offenen Methode der Koordinierung ab. Vorgesehen sind dabei rechtlich unverbindliche intergouvernementale Verfahren, die auf Benchmarking, Best-practices und freiwilliges Lernen setzen. Rechtlich verbindliche und an der Charta der Grundrechte orientierte Verfahren sind hingegen nicht vorgesehen, würden aber Parlamente stärker als bisher in die Ausgestaltung einer europäischen Cybersicherheitspolitik einbeziehen.

Die in der Cyberpolitik führenden fünf EU-Staaten setzen sich für eine ganzheitliche Strategie ein

Die Rolle der G-5

Während sich die EU-Institutionen vor allem auf die Sicherheitsaspekte konzentrieren, fordern die G-5 einen ganzheitlichen Ansatz. Vor diesem Hintergrund setzen sich die in der Cyberpolitik führenden fünf Mitgliedstaaten (G-5: Deutschland, Frankreich, Großbritannien, Niederlande und Schweden) in einem internen Papier vom Juli 2012 für eine ganzheitliche EU-Strategie im Cyberraum ein. So soll sich die EU-Strategie auf die ökonomischen und sozialen Aspekte, Infrastruktur, E-commerce und die Entwicklungszusammenarbeit konzentrieren. Folgt man diesem Ansatz, würde die von Ashton angestrebte Verankerung der Menschenrechte in der EU-Außenpolitik sich wie ein roter Faden durch die europäische Cyberstrategie ziehen. Sowohl der EU-Sonderbeauftragte für Menschenrechte, der europäische Datenschutzbeauftragte sowie die europäische Grundrechteagentur wären an der Ausarbeitung der EU-Strategie zu beteiligen.

Weiterhin fordert die G-5, dass der Datenschutz Eingang in die EU-Cybersicherheitsstrategie finden soll. Das ist das zentrale Anliegen der EU-Justizkommissarin Viviane Reding. Strengere Datenschutzvorgaben für soziale Netze und Institutionen soll es demnach künftig in ganz Europa geben. Soziale Netzwerke müssten Daten in Zukunft auf Wunsch ihrer Nutzer wieder löschen (das Recht auf Vergessen).

Grenzen der Selbstregulierung

Die Digitale Agenda zielt auf eine Ordnungsstruktur ab, die von einem Zusammenspiel zwischen staatlichen und nichtstaatlichen Akteuren (Unternehmen, Zivilgesellschaft, Wissenschaft und technische Community) gekennzeichnet ist. Dieses Zusammenspiel scheint als Ansatzpunkt zunächst unstrittig. Ein Informationsaustausch zwischen Sicherheitsbehörden, staatlichen Institutionen und nichtstaatlichen Akteuren ist schon deswegen unerlässlich, weil wesent-

liche Expertise ausschließlich in privater Hand liegt.

Hinzu kommt, dass ein Großteil dessen, was allgemein unter dem Begriff „kritische Infrastrukturen“ (Energie, Sicherheit, Verkehr) verstanden wird, sich im Besitz privater Anbieter befindet. Allerdings sind auch die zum Teil recht gegensätzlichen Interessen nicht zu übersehen. So stehen viele Unternehmen einer umfassenden Meldepflicht für Angriffe, der aus Gründen des Schutzes von kritischen Infrastrukturen nötigen Offenlegung von Sicherheitsstandards und verbindlichen staatlichen Regelungen sehr skeptisch gegenüber. Wenn der Einfluss Privater auf den Regelsetzungsprozess zu groß wird, befürchtet man, dass legitime öffentliche Anliegen ungenügend berücksichtigt werden. Freiwillige Verhaltenskodizes sind keine Garantie dafür, dass das öffentliche Interesse ausreichend gewahrt wird.

Bessere Exportkontrollen

Der Kommissionsvorschlag zielt darauf ab, die Kooperation zwischen den Mitgliedstaaten im Bereich der Sicherheitstechnologien in den nächsten Jahren zu intensivieren. Allerdings sollten hier zunächst die Exporteure von Informations- und Kommunikationstechnologie stärker politisch und juristisch in die Pflicht genommen werden. Autoritäre Staaten setzen immer mehr auf die Zensur, Überwachung und Kontrolle des Internets, was mit der Technologie von europäischen und nordamerikanischen Unternehmen wie Area in Italien, Ultimaco in Deutschland oder Blue Coat Systems in den USA ermöglicht wird.[3] Diese Technologien wurden in autoritären Staaten wie Syrien, Libyen, Bahrain, Tunesien, Iran oder Weißrussland eingesetzt, wobei davon auszugehen ist, dass solche Technologien in vielen weiteren autoritären Staaten eingesetzt werden.

Diese Entwicklung ist weder im strategischen Interesse Europas noch steht sie im Einklang mit den Zielen einer GASP, die Gefahren für die internationale Sicherheit und die Nichtverbreitung verhindern will. Eine europäische Harmonisierung der nationalen Rüstungsexportpolitiken wäre notwendig. Sie müsste auf die technischen Systeme ausgedehnt werden, die in der Lage sind, die Grundrechte von Internetnutzern zu schädigen oder die flächendeckende Überwachung von Internetnutzern zu ermöglichen.

Die Exporteure von Informations- und Kommunikationstechnologie sollten stärker in die Pflicht genommen werden

Die bisherige Kontrollpraxis des EU Code of Conduct und der Dual-use-Verfahren sind noch unzureichend. Das Europäische Parlament und die nationalen Parlamente sollten umfassend informiert und an Exportentscheidungen beteiligt werden. Andere sensible Sachverhalte werden auch in Ausschüssen des EP und des Bundestags unter Geheimhaltung behandelt.

[3] Ben Elgin und Vernon Silver: Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear-Bloomberg. Bloomberg 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

Breite öffentliche Beteiligung

Wie bereits deutlich wurde, ist die Cyberpolitik von einer Parlamentarisierung und ernsthafter Transparenz noch weit entfernt. Ein erster Schritt für eine breite öffentliche Beteiligung wäre der Beitritt der EU und ihrer Mitglieder zur Open Government Partnership-Initiative. Für die Initiative hatten sich im September 2011 auf Anregung der USA und Brasiliens 50 Staaten zusammengeschlossen. Konkret soll hiermit der Zugang zu amtlichen Dokumenten erleichtert werden. Eine generelle Veröffentlichungspflicht würde die demokratische Meinungs- und Willensbildung fördern, eine bessere Kontrolle staatlichen Handelns ermöglichen und damit einen Beitrag zur Korruptionsprävention leisten.

Eine generelle Veröffentlichungspflicht würde die demokratische Meinungs- und Willensbildung fördern

Die Cyberpolitik in der EU ist noch fest in der Hand der für die Innere Sicherheit zuständigen Institutionen. Die von der dänischen Ratspräsidentschaft vorgeschlagene Einführung des EU-Verfahrens „Gruppe der Freunde der Präsidentschaft zu Cyber“ sowie Vorschläge der G-5 zur Erarbeitung einer europäischen Cyberstrategie statt einer Cybersicherheitsstrategie weisen in die richtige Richtung, sind aber unzureichend. Notwendig sind rechtlich verbindliche Regelungen sowie die Einbindung nationaler Parlamente und des EP. Nur unter Berücksichtigung der politischen, sozialen und wirtschaftlichen Dimension des Internets über den Bereich der Sicherheit hinaus, mit rechtlich verbindlichen Regelungen sowie der Einbindung nationaler Parlamente und des EP lässt sich eine tragfähige europäische Strategie für das Internet entwickeln.

Dr. ANNEGRET BENDIEK ist wissenschaftliche Mitarbeiterin in der Forschungsgruppe „EU-Außenbeziehungen“ in der SWP.

BEN WAGNER ist Doktorand am Europäischen Hochschulinstitut in Florenz und Visiting Fellow beim ECFR in Berlin.

Deutsche Welle

»Wir bringen die Welt ein Stück näher«

Chi Viet Giang, Redaktion
Sevan Ibrahim-Sauer, Distribution

www.dw.de