Bendiek, Annegret; Dickow, Marcel; Meyer, Jens

Research Report

Europäische Außenpolitik und das Netz: Orientierungspunkte für eine Cyber-Außenpolitik der EU

SWP-Aktuell, No. 60/2012

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bendiek, Annegret; Dickow, Marcel; Meyer, Jens (2012) : Europäische Außenpolitik und das Netz: Orientierungspunkte für eine Cyber-Außenpolitik der EU, SWP-Aktuell, No. 60/2012, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/255080

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

SWP
1962–2012

Europäische Außenpolitik und das Netz

Orientierungspunkte für eine Cyber-Außenpolitik der EU

Annegret Bendiek / Marcel Dickow / Jens Meyer

Anfang Dezember 2012 verhandeln die Staaten der Vereinten Nationen über eine Novellierung des wichtigsten internationalen Vertragswerks für die globale Telekommunikation: der International Telecommunication Regulations. Den institutionellen Rahmen dafür bildet die International Telecommunication Union, eine Sonderorganisation der VN. Als größter Binnenmarkt der Welt hat sich gerade auch die Europäische Union in der internationalen Netzpolitik zu positionieren. Die derzeit in Arbeit befindliche Cyber-Strategie für die EU sollte den bestehenden Multistakeholder-Ansatz weiterentwickeln. Die Prinzipien der Netzneutralität sowie der Zugangs- und Nutzungsfreiheit gilt es in den Mittelpunkt einer europäischen Cyber-Außenpolitik zu stellen.

Im Dezember 2012 findet eine Versammlung der International Telecommunication Union (ITU) statt, bei der Vertreter aus 193 Ländern die International Telecommunication Regulations (ITRs) von 1988 neu verhandeln werden. Die Grenzen zwischen Internet und Telefonnetz haben sich längst verwischt: Das (leitungsvermittelte) Telefon-Festnetz wird auch zur Übertragung von (paketvermittelten) Internet-Daten verwendet; umgekehrt kann über das Internet telefoniert werden (Voice over IP). Telefonnetze sind praktisch als Teil des Internets zu betrachten. Die Digitalisierung und die paketvermittelte Übertragung von Daten auch in der Telefonie haben Infrastruktur und Endgeräte multifunktional werden lassen. Internetfähige Mobiltelefone machen die Unterscheidung zwischen Computer und Handy weitgehend hinfällig.

Wie die Telekommunikationsnetze global reguliert werden, ist in der Staatengemeinschaft durchaus strittig. Auch von der Positionierung der EU als größtem Binnenmarkt der Welt wird es abhängen, ob und wie dieser Konflikt gelöst werden kann.

Staatliche Netzmonopole

Wer die Telekommunikations-Infrastruktur kontrolliert, hat erheblichen Einfluss auf die Verbreitung von Informationen und Meinungen, die über diese Netze vermittelt werden. Staatliche Akteure wie Regierungen, Militär und Geheimdienste streben aus diesem Grund danach, Telekommunikationsnetze unter ihre Aufsicht zu bringen. Staaten mit einer schlechten Bilanz bei Menschen- und Bürgerrechten sind regel-

Dr. Annegret Bendiek ist wissenschaftliche Mitarbeiterin der Forschungsgruppe EU-Außenbeziehungen
Dr. Marcel Dickow ist wissenschaftlicher Mitarbeiter der Forschungsgruppe Sicherheitspolitik
Jens Meyer ist Webmaster der SWP

mäßig auch jene, die Internet und Mobilfunknetze am stärksten überwachen. Die Nichtregierungsorganisation »Reporter ohne Grenzen« zählt in ihrem Bericht von März 2012 folgende zwölf Staaten zu den »Feinden des Internets«: Bahrain, Belarus, Birma, China, Kuba, Iran, Nordkorea, Saudi-Arabien, Syrien, Turkmenistan, Usbekistan und Vietnam.

Vor allem autoritäre Regime kontrollieren das Internet und beschränken die Nutzung neuer Medien in ihrem Herrschaftsbereich. Zum Einsatz kommen dabei Maßnahmen wie die Sperrung einzelner Websites, manuelles oder automatisiertes Filtern des Datenverkehrs, Einschüchterung und Verhaftung von Netzaktivisten, Überwachung von Internet-Cafés, staatlich gesteuerte Hacker-Angriffe auf unliebsame Sites, Aufbau eines zensierten Intranets, Drosselung der Verbindungsgeschwindigkeit oder sogar zeitweiliges Abschalten des gesamten Internets innerhalb eines Staatsgebiets.

Wie weit die regionale Kontrolle von Infrastruktur und Datenverkehr gehen kann, zeigen Beispiele wie China und Iran. Die chinesischen Behörden kontrollieren und zensieren Blogs und andere Webseiten. Sie filtern den Inhalt der Datenpakete mittels einer Zensur-Software (»great firewall«) oder leiten den Datenverkehr von unliebsamen auf regimetreue Websites um. Westliche Online-Kommunikationsplattformen wie Google, Facebook und Twitter werden durch chinesische Angebote mit gleicher Funktion verdrängt. Im Iran entwickeln die Behörden ein eigenes, regimetreues Extranet unter staatlicher Aufsicht; verschlüsselte (SSL/HTTPS-) Verbindungen werden zugleich gesperrt.

Entgegen der landläufigen Auffassung, das Internet sei ein Netz gleichberechtigter Knoten, die einander beliebig ersetzen können, ist es durchaus verwundbar – nicht nur an den Übergängen (Gateways) zwischen seinen Subnetzen. Störungen von Seekabeln, Überlandleitungen oder Satellitenverbindungen können regionale Subnetze vom übrigen Internet trennen und damit die Erreichbarkeit von Netzadressen erheblich beschränken. Diese Schwachpunkte hat etwa das Mubarak-Regime während der politischen Umwälzungen in Ägypten ausgenutzt. In der Nacht vom 27. auf den 28. Januar 2011 wurde die nationale Netzinfrastruktur regelrecht abgeschaltet, indem man die Border Gateway Protocol Router – sozusagen das Verkehrsleitsystem – umprogrammierte. Damit waren die Datenverbindungen von und nach Ägypten unterbrochen (»Kill Switch«).

Ähnlich neuralgische Stellen besitzen auch Mobilfunknetze, etwa an den Durchleitungsstellen zu Drittanbietern. Zudem sind Mobiltelefonnetze zwar wabenartig in Funkzellen aufgebaut, aber streng hierarchisch strukturiert. Denn im Gegensatz zum Festnetz haben Mobilfunknetze eine zentrale Registratur (Home/Visitor Location Register), die sich dynamisch verändert, je nachdem, wo sich welches Mobiltelefon befindet. Diese Registratur-Server sind ein möglicher Angriffspunkt für Mobilfunknetze. Außerdem kann schon eine Unterbrechung der Stromversorgung von Handy-Masten zum »Kill Switch« für das Mobilfunknetz werden.

Im internationalen Netzaufbau sind solche »single points of failure« daher möglichst zu vermeiden. Wo sie sich aus technischen Gründen nicht verhindern lassen, sollten Alternativ-Verbindungen das Risiko entschärfen, dass sie als zentrale Angriffspunkte für einen »Kill Switch« genutzt werden.

Kommunikationsfreiheit im Internet erfordert, dass kein Akteur die alleinige Kontrolle über die Telekommunikationsnetze erlangt. Um die Netzneutralität zu bewahren, reicht es nicht aus, dass man staatliche und privatwirtschaftliche Monopole in der Telekommunikations-Infrastruktur verhindert – dies ist eine notwendige, aber noch keine hinreichende Bedingung. Denn ein Staat kann die Netze auf seinem Territorium unter Umständen auch dann kontrollieren, wenn es dort mehrere Telekommunikationsprovider

gibt. Erst wenn alternative Verbindungen bestehen, die dem Einfluss der Regierung entzogen sind, lässt sich die Verbreitung unliebsamer Informationen und Meinungen von staatlicher Seite nicht mehr unterbinden.

Vom Nutzen moderner Kommunikationsmittel

Spätestens mit dem Arabischen Frühling wurde die Frage virulent, inwieweit die Verfügbarkeit von multidirektionaler Massenkommunikation schon an sich eine emanzipatorische und demokratisierende Wirkung hat. Ob man die Umbrüche in Tunesien, Ägypten, Bahrain, Jemen und Syrien seit Dezember 2010 oder die Demonstrationen gegen Wahlfälschungen im Iran 2009 nun als Twitter- und Facebook-Revolutionen bezeichnen will oder nicht – gemeinsam ist diesen Ereignissen, dass eine kritische Protestmasse deshalb so rasch zusammenkam, weil die Aktivisten moderne Kommunikationsmittel nutzten. Freier Zugang zu Telekommunikationsnetzen ist zweifellos ein Faktor, der demokratische Entscheidungsprozesse begünstigt und die Zivilgesellschaft stärkt.

Positive Folgen hat ein ungehinderter Kommunikationszugang auch auf ökonomischem Gebiet. Die Marktwirtschaft profitiert, wenn Angebot und Nachfrage für Produzenten und Konsumenten gleichermaßen transparent sind. Monopolbildung, Manipulation und Korruption wird so entgegengewirkt. Nicht zuletzt ist Information selbst eine Handelsware und Informationstechnologie ein begehrter Exportartikel. Telekommunikationsnetze bilden damit eine politische und wirtschaftliche Infrastruktur, die für alle Bereiche der Außenpolitik strategische Bedeutung hat.

Neue Medien und Außenpolitik

Die neuen Techniken und Medien haben ein verändertes Kommunikationsverhalten ermöglicht. Der Informationsfluss ist nicht mehr uni-, sondern multidirektional. Jeder kann nicht nur Empfänger, sondern auch Sender von Daten sein. Eine bisher unerreichte Vielfalt an Informationen und Meinungen lässt sich in kürzester Zeit zu minimalen Kosten verbreiten. Neben den Berufs- ist der Gelegenheits-Journalist, neben Staats- und Privatfernsehen sind Videoplattformen wie YouTube und Vimeo getreten. Pressefreiheit ist nicht länger nur die Freiheit des Eigentümers einer Druckerpresse; neben der Zeitung existiert heute das Weblog (Blog). Wie gesehen, haben diese Innovationen auch eine politische Dimension. Aktuelle Überlegungen zur Rolle von neuen Medien in der europäischen Außenpolitik orientieren sich dabei maßgeblich an den USA und deren Erfahrungen mit Cyber-Außenpolitik.

Amerikanische Cyber-Demokratiepolitik

Im Bewusstsein der emanzipatorischen Potentiale neuer Medien hat US-Außenministerin Hillary Clinton bereits 2010 die Freiheit des Internets zu einem fundamentalen Prinzip amerikanischer Außenpolitik erklärt. Demnach soll kein Staat seinen Bürgern den Zugang zum Internet oder zu anderen technischen Kommunikationsmitteln verwehren. Die US-Regierung stellt finanzielle Mittel bereit, um in Ländern mit scharfer Zensur den Informationszugang zu verbessern.

Ein Bestandteil amerikanischer Cyber-Außenpolitik ist es, die Netzkontrolle autoritärer Regime zu unterlaufen. In Libyen etwa gelang es Rebellen im Frühjahr 2011 mit Hilfe Washingtons, Teile des nationalen Mobilfunknetzes zu übernehmen und für die Koordination ihrer Aktionen gegen das Gaddafi-Regime zu nutzen. Netzaktivisten entwickeln gegenwärtig mit Unterstützung der US-Regierung das »Internet in a Suitcase«, mit dem per WLAN (Wireless Local Area Network)-Vernetzung, Near Field Communication etc. eine lokale, staatsunabhängige Telekommunikations-Infrastruktur aufgebaut werden kann. Die amerikanische Regierung treibt auch den

Aufbau eines »Schatten-Mobilfunknetzes« in Afghanistan voran, für das Mobilfunkmasten auf Militärbasen der US-Armee installiert werden.

Nachteile der Schatteninfrastruktur

Mit einer solchen Schatteninfrastruktur gehen aber auch Gefahren einher. Erstens wird eine oppositionelle Gesinnung allein schon an der Nutzung der Parallelnetze ablesbar. Zweitens bieten diese einen zentralen Angriffspunkt, von dem aus die Kommunikation einer ganzen Gruppe getroffen werden kann. Drittens müssen die Betreiber einer Schatteninfrastruktur den Datenfluss über diese Netze zumindest so weit überwachen, dass sie eine Infiltration erkennen und verhindern können. Zudem wirkt eine wie auch immer geartete Zusammenarbeit mit dem Organisator des Schattennetzes – »dem Westen« – vielfach schon per se diskreditierend, setzt sie doch Oppositionelle dem Vorwurf aus, Marionetten fremder Mächte zu sein. Eine Schatteninfrastruktur kann daher zwar temporär weiterhelfen, sie bietet aber keine dauerhafte Lösung der Probleme politischer Kommunikation in autoritär regierten Staaten.

Sinnvoller erscheint es, wenn freiheitliche Staaten eine ungehinderte Kommunikation über den von ihnen kontrollierten Teil des Internets ermöglichen und nicht nur in separaten Subnetzen. Dazu gibt es bereits Projekte wie TOR (»The Onion Router«) oder »Telex«. Demokratien stehen dabei allerdings vor einem Dilemma. Technische Verfahren, um sich staatlicher Überwachung zu entziehen, können Freiheitsbewegungen ebenso zugutekommen wie terroristischen Gruppierungen. Westliche Polizeibehörden und Geheimdienste fordern daher eine – auch grenzüberschreitende – Ausweitung ihrer Kontrollbefugnisse. Die Internet-Freiheit im eigenen Land ist jedoch ein Maßstab für die Glaubwürdigkeit von Cyber-Außenpolitik. Doppelte Standards zwischen In- und Ausland würden diese Glaubwürdigkeit untergraben.

Wenn westliche Anbieter von Netz-Hardware autoritären Staaten die Überwachungstechniken gleich mitliefern, läuft dies dem Bestreben zuwider, undemokratische Regime an der Kontrolle und Zensur ihrer »Untertanen« zu hindern. Zu empfehlen sind daher Maßnahmen wie ein generelles Verbot, Filter- und Zensurtechnologie in solche Länder zu exportieren. Zwar haben 2009 verschiedene US-Unternehmen (darunter Yahoo, Google und Microsoft), Forschungsinstitute und Menschenrechtsgruppen mit der »Global Network Initiative« einen Kodex beschlossen, der dazu verpflichtet, bei Geschäften mit autoritären Staaten bestimmte Richtlinien einzuhalten. Darunter fällt vor allem, die Meinungsfreiheit zu achten, die Privatsphäre zu schützen und Behörden nicht bei entsprechenden Restriktionen zu unterstützen. Die meisten Netzausrüster fehlen jedoch bei dieser Initiative.

EU-Initiativen

In der EU laufen derzeit mehrere Abstimmungsprozesse, mit denen Europas künftige Cyber-Politik festgelegt wird. Der Europäische Rat hat mit dem Implementierungsbericht zur Europäischen Sicherheitsstrategie die EU-Akteure bereits im Dezember 2008 aufgefordert, ein »umfassendes Konzept« für die Cyber-Politik zu erarbeiten. Dabei wurde allerdings nicht präzisiert, ob es sich um eine Cyber-Außenpolitik oder eine Cyber-Sicherheitsstrategie handeln soll. Im Zuge des Arabischen Frühlings und der entsprechenden US-Initiativen organisierte die britische Regierung im November 2011 eine erste größere Konferenz zur Normen-Entwicklung im Cyber-Raum. Zur Vorbereitung entwickelten die drei EU-Kommissarinnen Neelie Kroes (DG Connect), Cecilia Malmström (DG Home Affairs) und Catherine Ashton (Hohe Vertreterin für Außen- und Sicherheitspolitik, Vizepräsidentin der Kommission) im Oktober 2011 ein »Food for Thought Paper« über Verhaltensnormen im Cyber-Raum.

In Dokumenten, die der Europäische Auswärtige Dienst später zur Cyber-Sicherheit vorgelegt hat (Juni 2012, Oktober 2012), steht das von Ashton postulierte Mainstreaming von Menschenrechten in der Außen- und Sicherheitspolitik an prominenter Stelle. Dagegen wird diesem Punkt im Kommissionsvorschlag »Communication on European Strategy for Cyber Security« von Ende Mai 2012 nur nachrangige Bedeutung zugemessen. Der Vorschlag erklärt es zum Ziel, ein sicheres digitales Umfeld für Bürger, Unternehmen und Verwaltungen herzustellen und Cyber-Kriminalität zu verhindern. Die EU plant unter anderem die Verbesserung ihrer Cyber-Verteidigungsfähigkeit, die Schaffung eines gemeinsamen Marktes für Sicherheitstechnologie, die Förderung zwischenstaatlicher Kooperation sowie weitere Maßnahmen zu Aufklärung und Forschung.

Der Kommissionsvorschlag versteht die Telekommunikationsnetze vor allem als Tatort für Cyber-Kriminalität, -spionage und -sabotage, kurz: als Sicherheitsproblem und Gefahrenquelle. Dementsprechend behandelt er überwiegend die Frage, wie der Staat und die EU sich vor Bedrohungen aus dem Internet schützen können. Andere Gesichtspunkte dagegen drohen ins Hintertreffen zu geraten – etwa Datenschutz, informationelle Selbstbestimmung, Schutz des Bürgers vor staatlicher Überwachung, aber auch die positiven Effekte der Netze für Beschaffung und Verbreitung von Informationen, für Open Government, Meinungsfreiheit, Pluralismus und Marktwirtschaft.

Die europäische Grundrechteagentur, der Europäische Datenschutzbeauftragte und der Sonderbeauftragte für Menschenrechte sollten daher in die Ausarbeitung einer EU-Strategie eingebunden werden. Justizkommissarin Viviane Reding, die sich gegenwärtig bemüht, ein übergreifendes Datenschutzrecht zu schaffen, wäre im Sinne einer umfassenden Strategie für den Cyber-Raum ebenfalls zu beteiligen.

Die Rolle der Cyber-G5

Die in der Cyber-Politik führenden fünf EU-Mitgliedstaaten (Cyber-G5: Deutschland, Frankreich, Großbritannien, Niederlande und Schweden) haben im Juli 2012 auf Druck Schwedens und der Niederlande eine Cyber-Strategie vereinbart, die über den Bereich Sicherheit hinausgeht. Sie soll ökonomische und soziale Elemente, Aspekte der Infrastruktur und des e-commerce sowie die Entwicklungszusammenarbeit integrieren. Richtungsweisend sind hier auch e-diplomacy-Initiativen, die ihren Ursprung in den Vereinigten Staaten haben.

Angesichts der zahlreichen EU-Initiativen in diesem Bereich sollte eine künftige Strategie der Union als Scharnier zwischen den Mitgliedstaaten und der internationalen Ebene fungieren. Zugleich müsste sie selbstverständlich auch nach innen wirken.

Weiterentwicklung des Multistakeholder-Ansatzes

Auf der anstehenden Konferenz der International Telecommunication Union werden gegensätzliche Haltungen in der Frage von Netz-Regulierung aufeinandertreffen. Einige afrikanische und asiatische Staaten wollen die Kontrolle regionaler Subnetze in die Hände staatlicher Autoritäten legen. China, Russland, Usbekistan und Tadschikistan – Mitglieder der sogenannten Shanghai-Gruppe – haben 2011 vorgeschlagen, einen zwischenstaatlichen »Internationalen Verhaltenskodex für Informationssicherheit« zu verabschieden. Nach diesem Kodex soll die von Aktivitäten im Internet bedrohte Souveränität des Staates gestärkt und jede Einmischung in dessen innere Angelegenheiten verboten werden. Weiter schwebt den Initiatoren vor, die ITU institutionell zu stärken, die International Telecommunication Regulations zu überarbeiten und die Vergabe von Internet-Domains – die derzeit beim US-Unternehmen Internet Corporation for Assigned Names and Numbers (ICANN) angesiedelt ist – auf die ITU zu übertragen.

Aus Sicht westlicher Länder wäre dies ein Einfallstor für staatliche Zensur. Sie setzen eher auf eine Selbstregulierung der Netze durch private Betreiber; den chinesisch-russischen Vorschlägen steht dabei das von USA und EU präferierte Multistakeholder-Modell gegenüber. Dieses sieht vor, all jenen eine Teilhabe an der Internet-Regulierung zu ermöglichen, die entweder über relevantes Expertenwissen (Unternehmen, Wissenschaft), politische Autorität (Staaten) oder über gesellschaftliche Legitimation (Zivilgesellschaft) verfügen. Mit Skepsis betrachten die Vertreter dieser sehr viel pluralistischeren Regulierung sowohl eine starke Rolle der VN als auch verbindliche zwischenstaatliche Verträge. Die im Mai 2011 von US-Präsident Obama verkündete »International Strategy for Cyberspace« setzt denn auch darauf, transnationale Dialoge über Verhaltensnormen, vertrauensbildende Maßnahmen und die Einbindung nichtstaatlicher Akteure zu intensivieren. Einen internationalen Vertrag hingegen lehnen die USA ab – dieser sei zu starr, so die Argumentation, zu wenig verifizierbar und zu sehr auf staatliches Handeln ausgerichtet.

Keine der beiden Positionen kann überzeugen. Während der russisch-chinesische Vorschlag einseitig auf die Ausdehnung staatlicher Kontrollmacht zielt, vertritt das Multistakeholder-Modell fast ausschließlich die Interessen der OECD-Staaten, insbesondere der technologisch überlegenen USA und global agierender Unternehmen.

Auch nichtstaatliche Stakeholder bieten keine hinreichende Gewähr für eine freie und ungehinderte Kommunikation im digitalen Raum. Sie verfolgen eigene, kommerzielle Interessen, die der Gleichberechtigung aller Netz-Nutzer durchaus entgegenstehen können. Zudem gelingt es solchen Akteuren nur selten, sich staatlichem Einfluss entziehen, zumal in autoritären Ländern. Aus wirtschaftlichem Interesse versuchen auch Unternehmen oder private Netzbetreiber, Monopole zu schaffen oder die Verfügbarkeit von Daten einzuschränken, indem sie etwa proprietäre Plattformen schaffen und diese vom übrigen Internet abschotten. Dies gilt für Hersteller und Anbieter von Hard- und Software, aber auch für die Betreiber sozialer Netzwerke wie Facebook und Konzerne wie Google.

Fazit für die europäische Politik

Die EU-Strategie sollte an das Europarats-Übereinkommen zur Computerkriminalität anknüpfen, das 2001 in Budapest unterzeichnet wurde und 2004 in Kraft trat. Ziel sollte sein, die Vereinbarung vollständig umzusetzen und dieses Modell auf die internationale Ebene zu übertragen. Das Budapest-Übereinkommen bildet eine konstruktive Grundlage für eine engere Zusammenarbeit zwischen den Mitgliedstaaten des Europarates sowie einigen außereuropäischen Staaten wie den USA, Japan und Kanada. Die bestehende Architektur des Internets mit seinen offenen Standards und einer dezentralen Verwaltung sollte beibehalten werden. Hinzutreten sollte ein Instrument zur Förderung rechtlicher Verbindlichkeit. Bei Verstößen könnten Sanktionen durch den VN-Sicherheitsrat verhängt werden. Zudem wäre das bestehende Multistakeholder-Modell weiterzuentwickeln. Bei der Formulierung neuer Regeln sollte dabei die Expertise privater Akteure genutzt werden, während diese gleichzeitig darauf festzulegen sind, globale Standards in den Bereichen Sicherheit, informationelle Selbstbestimmung und Datenschutz einzuhalten.

Die Cyber-Strategie der EU sollte sich aber nicht nur auf die Computer-Kriminalität konzentrieren, sondern auch die emanzipatorischen Aspekte der Telekommunikation in den Blick nehmen. Im Zentrum europäischer Cyber-Außenpolitik sollten Prinzipien der Zugangs- und Nutzungsfreiheit stehen. Die richterliche Kontrolle durch den Europäischen Gerichtshof wäre auszubauen, um Monopolbildung zu sanktionieren und die Netzneutralität sowie die Zugangs- und Nutzungsfreiheit in der EU zu gewährleisten.

Wichtige Prinzipien, auf die eine europäische Cyber-Außenpolitik ausgerichtet sein sollte, sind:

- Zugangsfreiheit: Chancengleichheit und Nicht-Diskriminierung beim Zugang zur Telekommunikations-Infrastruktur (Inklusivität)
- Netzneutralität: Die EU sollte sich dafür einsetzen, dass die Telekommunikations-Infrastruktur sich neutral gegenüber allen von ihr transportierten Informationen verhält, dass einzelne Datenpakete also weder aus finanziellen noch aus politischen Gründen gegenüber anderen bevorzugt oder benachteiligt werden.
- Vertraulichkeit der Kommunikation mittels Verschlüsselung der Inhalte und Schutz der Kommunizierenden vor staatlicher Repression durch ein universelles Recht auf Anonymität: Die Möglichkeit, die Identität von Kommunizierenden zu verschleiern, muss besonders bei der schon laufenden Einführung des neuen Internet-Protokolls Version 6 (IPv6) berücksichtigt werden. Bei diesem Verfahren müssen IP-Adressen nämlich nicht mehr dynamisch vergeben werden; vielmehr hat jeder Netzknoten eine eindeutige, permanente IP-Adresse, was den Schutz der Anonymität zumindest erheblich erschwert.

Diese Prinzipien sind international nicht leicht durchsetzbar. Doch immerhin gibt es vielfältige Möglichkeiten, sich für demokratische und rechtsstaatliche Standards einzusetzen – bei der (Außen-) Wirtschaftsförderung, bei der Ausgestaltung bilateraler oder multilateraler Abkommen, im Bereich von Bildung und Ausbildung oder im Exportrecht.

Die künftige Cyber-Außenpolitik der EU könnte sechs konkrete Maßnahmen ergreifen:

- Länder, in die Gelder aus staatlichen oder EU-Hilfsfonds fließen (z.B. durch Entwicklungshilfe, Nachbarschaftsprogramme, Strukturfonds, Bürgschaften oder Kredite), werden im Gegenzug verpflichtet, mehr Pluralität im Bereich der Netze und Netzbetreiber zu schaffen.
- Exporte von Überwachungstechnik werden EU-weit kontrolliert und beschränkt, Überwachungsverfahren dem Kriegswaffenkontrollgesetz unterstellt.
- Auf EU-Ebene wird die Ausfuhr von Dual-Use-Gütern im Bereich der Telekommunikation rechtlich verbindlich durch das Europäische Parlament kontrolliert.
- EU-einheitlich werden Kryptographie und andere Selbstschutzmaßnahmen gefördert und zum Export freigegeben. Wo Verschlüsselung noch unter Kriegswaffenkontrolle steht, wird dies aufgehoben.
- Das Internet als Allmende (Commons): Zum Schutz der Netz-Infrastruktur werden – auch im Rahmen der ITU – internationale Vereinbarungen abgeschlossen, die völkerrechtlich bindend sind (nach dem Vorbild von Weltraumvertrag oder Antarktisvertrag). Internationale Verträge ächten, dass staatliche oder privatwirtschaftliche Akteure eine alleinige Kontrolle über die Telekommunikations-Infrastruktur ausüben.
- Die Internet-Alphabetisierung wird zu einem Schwerpunkt der EU-Entwicklungsziele gemacht; entsprechende Bildungsprogramme in Krisengebieten werden von der EU unterstützt oder selbst aufgelegt.

Bei den ITU-Verhandlungen im Dezember 2012 und darüber hinaus sollte der Schutz der Privatsphäre vor Eingriffen staatlicher Stellen und privater Akteure im Vordergrund stehen. Im multilateralen Kontext bietet es sich an, den Internationalen Pakt über bürgerliche und politische Rechte (ICCPR) zu modifizieren. Konkret sollte das General Comment zu Artikel 17 aktualisiert werden, in dem das Recht auf Privatsphäre verankert ist. Eine solche rechtsverbindliche Interpretation des internationalen Menschenrechtsschutzes der Privatsphäre hat zuletzt 1988 stattgefunden. Verantwortlich dafür sollte künftig der VN-Menschenrechtsausschuss sein.

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 1611-6364