Cybersicherheit - eine facettenreiche politische Herausforderung: aus internationalen Zeitschriften 2012/2013

Bendiek, Annegret; Ulmer, Kathrin

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Zeitschriftenschau

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Cybersicherheit – Eine facettenreiche politische Herausforderung

Aus internationalen Zeitschriften 2012/2013

Annegret Bendiek / Kathrin Ulmer

Die jüngsten Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden haben dafür gesorgt, dass Cybersicherheit in den Mittelpunkt der öffentlichen Debatte rückte. Wie nimmt sich die politikbegleitende Wissenschaft dieses Themas an? Ein Blick in neuere Beiträge internationaler Zeitschriften zeigt, dass unter dem Schlagwort Cybersicherheit sehr unterschiedliche Aspekte diskutiert werden, etwa die Cyber-Abschreckung als Mittel gegen Cyberangriffe, die Internet-Governance oder der Nutzen digitaler Diplomatie als präventives Instrument für mehr Cybersicherheit. Die Fachbeiträge spiegeln die verschiedenen Facetten eines neuen Politikfelds der Außen- und Sicherheitspolitik wider. Der Mehrwert der noch sehr jungen wissenschaftlichen Fachdiskussion ist vor allem darin zu sehen, dass sie viele Fragen aufwirft, die Entscheidungsträger in Politik und Wirtschaft im Umgang mit Cyberrisiken beantworten müssen.

Spätestens seit den Enthüllungen des US-amerikanischen Ex-NSA-Mitarbeiters Edward Snowden ist Cybersicherheit in aller Munde. Um über die Medienberichterstattung hinaus den Blickwinkel zu erweitern, bietet es sich an, die wissenschaftliche Bearbeitung des Themas zu untersuchen. Anders als in den Medien ist in der wissenschaftlichen Literatur schon der Begriff Sicherheit selbst umstritten. Wenn es um Cybersicherheit gehe, fehle es laut **Gustav Lindstrom**, Leiter des *Euro-Atlantic Security Programme* am *Geneva Centre for Security Policy* (GCSP), an international anerkannten Definitionen für viele Begriffe, die in der Debatte zentral seien, etwa Cyberkriminalität, Cyberkrieg und Cyberterrorismus. Die Frage, welche Bedingungen erfüllt sein müssen, um einen Cyberangriff als bewaffneten Angriff im Sinne des Völkerrechts einstufen zu können, sei genauso unbeantwortet wie diejenige, welche Rechte Opfer solcher Attacken haben. Außerdem beobachtet Lindstrom einen Trend zur offensiven Nutzung von Cybertechnologien, den es zu bedenken gelte. Die Diskussion um Cybersicherheit solle sich auf die Frage nach angemessenen politischen und rechtlichen Maßnahmen konzentrieren, mit deren Hilfe der Einsatz von Cyberwaffen

Dr. Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU-Außenbeziehungen
Kathrin Ulmer ist Forschungsassistentin in der Forschungsgruppe EU-Integration

begrenzt werden könnte. Cyberangriffsfähigkeiten entwickelten sich, so Lindstrom, immer mehr zu einem strategischen Instrument zwischenstaatlichen Konfliktaustrags. Außerdem müssten sich politische Akteure um die Verständigung über ein Modell der Internet-Governance bemühen; sei es, den derzeitigen Modus beizubehalten, sei es, eine stärkere Regulierung einzuführen, wie insbesondere China und Russland es wünschen.

Eine ebenfalls lohnende Lektüre zur Einordnung von Cybertechnologien und zu ihrer Neuartigkeit für die Außen- und Sicherheitspolitik bietet der Beitrag von **James A. Lewis**, Senior Fellow und Direktor des *Technology and Public Policy Program* am *Center for Strategic and International Studies* (CSIS), den er für die Zeitschrift *Military and Strategic Affairs* verfasste. Seit den 80er Jahren würden Cybertechniken von den Geheimdiensten eingesetzt, aber erst seit den 90er Jahren seien militärische Cyberangriffe festzustellen. Cyberattacken böten neue Mittel und Wege zur zwangsweisen Interessensdurchsetzung (coercion) und Spionage, seien aber nicht als neue Konfliktkategorie einzustufen. Es sei falsch, die Schadprogramme *Stuxnet* und *Flame* als Merkmale einer neuen Art von Kriegsführung darzustellen; auch hätten derartige Angriffe nicht die Zerstörungsgewalt von Nuklearwaffen. Die Einordnung von *Stuxnet* als Mittel zur Kriegsführung erschwere sogar die internationalen Verhandlungen, in denen der Cyberspace verregelt werden solle. Hochentwickelte Cybertechniken à la *Stuxnet* stünden derzeit allein den USA, dem Vereinigten Königreich, Israel, Russland und China zur Verfügung. Andere Staaten beabsichtigen, sich ähnliche Fähigkeiten anzueignen. Bislang sind Angriffe mit großen physischen Schäden ausgeblieben. Fraglich sei allerdings, so Lewis, ob dies so bliebe, wenn Staaten wie Iran und private Akteure über ausreichende Cyberangriffsfähigkeiten verfügten. Lewis plädiert dafür, den größeren geopolitischen Kontext von Cyberattacken im Blick zu behalten: So beobachtet er, dass die Enthüllungen um die Spionagesoftware *Flame* durchaus Russlands Verhandlungsposition in Fragen der Internet-Governance und Cybersicherheit gedient haben könnten.

Cyber-Abschreckung am Beispiel der USA

Myriam Dunn Cavelty, Leiterin der *Risk & Resilience Research Group* am *Center for Security Studies* an der ETH Zürich, analysiert in ihrem Beitrag in der *International Studies Review*, wie die militärische Sprache im Zuge sicherheitsrelevanter Cybervorfälle die Oberhand gewinnt. Cybersicherheit werde vorwiegend als militärisches Problem gesehen, das von militärischen Akteuren zu lösen sei. Dunn Cavelty stellt diese Verknüpfung in Frage und mahnt, derartige scheinbar unzweifelhafte Zusammenhänge immer wieder zu hinterfragen. **Frank J. Cilluffo**, Direktor des *Homeland Security Policy Institute* (HSPI) und Ko-Direktor des *Cyber Center for National and Economic Security* (CCNES) an der George-Washington-Universität in Washington, D.C., **Sharon L. Cardash**, Associate Director des HSPI und Mitglied des CCNES, und **George C. Salmoiraghi**, Anwalt und Berater des HSPI, hinterfragen dagegen nicht. Sie stellen in der Zeitschrift *Military and Strategic Affairs* Eckpunkte für eine Cyber-Abschreckungsstrategie (Cyber-Deterrence) der USA vor. Zum Schutz kritischer Infrastrukturen wie etwa Wasser- und Stromversorgung empfehlen die Autoren den USA, eine Cyber-Abschreckungsstrategie zu formulieren. Die Vereinigten Staaten sollten in der Cyberpolitik Führungswillen demonstrieren und einem konkreten Aktionsplan folgen. Kernpunkte amerikanischer Hegemonie lägen nicht nur darin, die eigene militärische Stärke auszubauen oder einen Erstschlag zu führen, sondern auch, einem Cyberangriff nahezu in Echtzeit militärisch begegnen zu können. Hierzu müsse die technologische und wissenschaftliche Führungsposition der USA bewahrt werden. Ziele und Motive potentieller Angreifer sollten schnell identi-

fiziert werden, um angemessene Gegenmaßnahmen ergreifen zu können. Trotz des immensen technologischen Fortschritts bei gleichzeitiger Informationsknappheit hinsichtlich Tätern und Motiven müsse die US-Regierung deren technologischen Fähigkeiten standhalten können. Nach Ansicht der Autoren sollten stärkere Anreize für den Privatsektor gesetzt werden, kritische Infrastruktur zu schützen. Auch Kooperation mit internationalen Verbündeten im Cyberbereich sei notwendig.

Noch vor Edward Snowdens Aussagen zu den Überwachungsprogrammen *Prism* und *Tempora* übte der amerikanische Journalist **James Bamford** in einem vielbeachteten Aufsatz im Magazin *Wired* Kritik an der gegenwärtigen US-Cyberpolitik. Bamford schreibt seit mehreren Jahrzehnten über die NSA. Er legt dar, wie diese unter der Führung von General Keith Alexander ihre Internetüberwachungsprogramme ausgeweitet hat, ohne dass dazu je eine politische Debatte über die gesellschaftlichen Konsequenzen stattgefunden hätte. Cybersicherheit aus offizieller Sicht der USA bedeute, so Bamford, dass das Pentagon ungeachtet aller Haushaltskürzungen 4,7 Milliarden US-Dollar für »Operationen im Cyberspace« für 2014 beantragt habe, etwa eine Milliarde mehr als der Vorjahres-Etat. Ein beträchtlicher Anteil werde der Cybereinheit unter General Alexander zur Verfügung gestellt. Hiermit solle der Aufbau von 13 Cyberangriffsteams finanziert werden. Für die US-Regierung verursachten sogenannte *Zero-Day-Exploits*, die in falsche Hände geraten, eine große Sicherheitslücke, die es zu schließen gelte. Bei einem *Zero-Day-Exploit* handelt es sich laut dem Softwareunternehmen Kaspersky Lab um eine »Schadsoftware, die am gleichen Tag erscheint wie die Entdeckung des Bugs [eines Programmfehlers, Anm. d. Verf.] oder der Sicherheitslücke in der Anwendung oder im Betriebssystem, welche durch den Exploit ausgenutzt wird. Dem Hersteller bleibt keine Zeit, ein Patch [eine Korrektursoftware, Anm. d. Verf.] bereitzustellen, und auch IT-Administratoren kommen nicht dazu, rechtzeitig andere Abwehrmechanismen einzusetzen«. Angriffe, die solche Schwachstellen ausnutzen, seien gleichsam die »Achillesferse des Sicherheitsbusiness«, wie ein ehemaliger Geheimdienstmitarbeiter bei Bamford zitiert wird. Entsprechend hoch seien die Summen, die Akteure für *Zero-Day-Exploits* bezahlen Daraus entwickle sich laut Bamford ein gefährliches und unreguliertes Cyberwettrüsten mit eigenen Grau- und Schwarzmärkten.

Normen-Regression und die Rolle der BRICS

Während einige Sicherheitsexperten den Ausbau staatlicher Cyberangriffsfähigkeiten befürworten, beobachten andere Wissenschaftler in der Internet-Governance die Tendenz zur Versicherheitlichung auf Kosten von Freiheitsrechten. So konstatieren **Ronald J. Deibert**, Direktor des *Canada Centre for Global Security Studies* und des *Citizen Lab* an der *Munk School of Global Affairs* an der Universität Toronto, und **Masashi Crete-Nishihata**, Forschungsmanagerin am *Citizen Lab*, in ihrem Artikel für die Zeitschrift *Global Governance* eine »Normen-Regression« globaler Governance. Dies bedeute, dass immer mehr Regeln aufgestellt werden, die den Cyberspace als »offenes Gemeingut der freien Information und Kommunikation« (open commons of information and communication) einschränken. Hier handle es sich um eine Entwicklung zurück zu traditionellen Formen staatlicher Kontrolle. Zu den staatlichen Informationskontrollen zählen Zensur sowie Einschränkung oder Unterbrechung des Internetzugangs, um Proteste oder Unruhen zu verhindern. Als Foren, die Kontrollnormen förderten, identifizieren die Autoren die *International Telecommunications Union* (ITU) oder regionale Organisationen wie die *Shanghai Cooperation Organization* (SCO). Vereinfacht werde staatliche Zensur auch durch den Im- und Export einschlägiger Technologie, so für Cybersicherheit, kom-

merzielle Internetfilter, Überwachung oder offensive Operationen.

Warum Multilateralismus so schwer zu bewerkstelligen ist und welche Rolle die BRICS-Staaten (Brasilien, Russland, Indien, China, Südafrika) in der Internet-Governance und Cybersicherheit spielen, erläutern **Hannes Ebert** und **Tim Maurer** in der Zeitschrift *Third World Quarterly*. Gemeinsam sei allen BRICS-Staaten, dass sie den USA kritisch gegenüberstünden und aktiv gegen deren Vormachtstellung vorgingen. Allerdings unterschieden sich ihre außenpolitischen Strategien. Russland und China favorisierten staatliche Kontrolle in der Internet-Governance und wollten internationale Koordination über die *ITU* regeln lassen. Beide strebten einen zwischenstaatlich organisierten *International Code of Conduct for Information Security* an. Indien, Brasilien und Südafrika (IBSA) dagegen bevorzugten ein »intergouvernementales« Modell mit dem Ziel, die Regelsetzung in der Internet-Governance über eine eigens hierfür geschaffene internationale Organisation zu ermöglichen, die aber auch wichtige nichtstaatliche Stakeholder einschließe. Die IBSA-Staaten seien gegen Internetzensur und geschlossene Netzwerke, positionierten sich aber auch als »Swing States« in der globalen Debatte. Uneinheitliches Verhalten der BRICS-Staaten in diesem Kontext sei auch darauf zurückzuführen, dass einige dieser Staaten Demokratien sind, andere aber nicht. Laut den Autoren spielen aber auch weitere Faktoren hier eine gewichtige Rolle: erstens unterschiedliche historische Erfahrungen, die das Verhältnis von Bürger und Institutionen prägten, zweitens die Mobilisierungskraft von Zivilgesellschaften durch soziale Medien, drittens die Kopplung von Informationssicherheit mit der Menschenrechtsdebatte und viertens der Aufstieg Chinas, der den aufstrebenden Staaten Anlass biete, sich von den USA zu emanzipieren und ihre Interessen gegenüber anderen aufsteigenden Mächte abzugrenzen. Als Beispiel für den vierten Punkt wird die Zusammenarbeit Indiens oder Brasiliens mit den USA in der Internet-Governance und Cybersicherheit genannt.

Digitale Diplomatie

Die Rolle von Public Diplomacy erörtert **Nicholas J. Cull**, Professor für *Public Diplomacy* an der *University of Southern California* in Los Angeles, in seinem Artikel für die Zeitschrift *International Studies Review*. Er zeichnet nach, wie moderne Informations- und Kommunikationstechnologien in der US-amerikanischen Public Diplomacy eingesetzt wurden, beschreibt also den Dialog mit zivilgesellschaftlichen Akteuren in Drittstaaten. Zuständig hierfür war seit 1953 die aus Culls Sicht ausgesprochen innovative *US Information Agency*, bevor 1999 das Außenministerium diese Aufgabe übernahm. Dieses habe, beklagt der Autor, informationstechnische Mittel zunächst nur sehr zurückhaltend verwendet, indem es lediglich Nachrichten verbreitet habe. Erst Enthüllungen durch WikiLeaks und die Umbrüche in der arabischen Welt seit Dezember 2010 hätten bewirkt, dass von den Dialogmöglichkeiten der Informationstechnik ausgiebiger als zuvor Gebrauch gemacht worden sei. Diplomatie müsse in digitalen Foren und weiteren individuell genutzten Kanälen aktiver werden. »Public Diplomacy 2.0« folge der Idee eines horizontalen Netzwerks, das soziale Netzwerke und Online-Communities einbeziehe.

Marietje Schaake, niederländische Europaabgeordnete in der liberaldemokratischen Fraktion, geht in ihrem Artikel für die Zeitschrift *Security and Human Rights* noch weiter. Sie hebt den Wert der digitalen Freiheitsrechte ebenso hervor wie die Verantwortung, die daraus für die EU-Diplomatie erwachse. Der Arabische Frühling habe die demokratiefördernde Wirkung moderner Informations- und Kommunikationstechnologie offenbart. Hier stehe der EU ein Demokratisierungshebel zur Verfügung. Wie Cull unterstreicht auch Schaake die Macht, die Individuen durch Technologie erhielten. Nach Ansicht der

Autorin müsse sich europäische Politik für das digitale Zeitalter erneuern, um dem europäischen Anspruch zu Schutz und Durchsetzung von Menschenrechten genügen zu können. Die EU-Diplomatie müsse ihre Politik dem digitalen Zeitalter anpassen, etwa indem sie Oppositionelle in autoritären Regimen dazu befähige, ihre Freiheitsrechte wahrzunehmen und Zensur zu umgehen, oder indem sie den Export von Technologien verhindere. Digitale Freiheitsrechte förderten auch traditionelle Menschenrechte wie Meinungs- und Versammlungsfreiheit. Schaake propagiert in ihrem Beitrag eine menschenrechtsorientierte Cyberaußenpolitik, die die zentrale Bedeutung der Privatwirtschaft anerkennt und verlangt, dass diese sich europäischen Werten gemäß verhält. Außerdem sollten digitale Freiheitsrechte in der EU selbst geschützt werden, damit die Union glaubwürdig bleibe und ihre Vorbildfunktion erfüllen könne. Gerade in dieser Hinsicht werde die EU von außen intensiv beobachtet. Zwar sieht Schaake die Risiken der Digitalisierung für die Außen- und Sicherheitspolitik. Gleichwohl müsse Informations- und Kommunikationstechnologie dazu dienen, auch in Demokratien selbst Freiheits- und Menschenrechte durchzusetzen.

Cybersicherheit hat großen Einfluss auf Freiheitsrechte, doch dies ist auch umgekehrt der Fall. Dieses Wechselverhältnis nimmt **Steven C. Bennett** in seinem Fachbeitrag »The Right to Be Forgotten« im *Berkeley Journal of International Law* kritisch unter die Lupe. Hiermit ist das Recht der Internetnutzer gemeint, Daten kontrollieren und vollständig löschen lassen zu können. Bennett skizziert die Bemühungen zum Datenschutz, die Europa in dieser Hinsicht seit 2010 unternommen hat. Dazu gehören die Regeln, die alle in der EU operierenden Unternehmen befolgen sollen. In den USA dagegen werde das Recht auf freie Meinungsäußerung höher eingeschätzt als der Datenschutz. Anders als in der EU lege man in den Vereinigten Staaten zudem wenig Wert darauf, dass sich die Regierung für den Datenschutz stark mache. Da die Wirtschaft heute internetbasiert sei, komme laut Bennett der Harmonisierung internationaler Datenschutzrichtlinien eine Schlüsselrolle zu. Neueren Entwicklungen in den USA seit 2010 sei zu entnehmen, dass die USA mittlerweile größere Offenheit für Datenschutzfragen und auch für den Dialog mit EU-Behörden an den Tag legten. Dieser Dialog würde durch einen einheitlichen EU-Datenschutzstandard erheblich vereinfacht, sodass beide Partner zumindest auf Minimalstandards für ein »Right to Be Forgotten« hinarbeiten könnten. Trotz dieser Fortschritte bleibe die Frage, wie rechtlich mit bestehenden Datenschutzkonflikten umzugehen sei. Ungewiss sei vor allem, wie weit der Kompetenzbereich der EU-Gerichte im Hinblick auf solche Akteure reiche, die außerhalb der EU operierten, deren Tätigkeit aber Auswirkungen auf die EU hätte. Angesichts solcher Fragen im grenzenlosen Cyberspace erweise sich die traditionelle Konzeption einer Gerichtsbarkeit, die auf der Souveränität über ein bestimmtes Territorium beruhe, als besonders problematisch. Zwar sei es laut Bennett ein ehrgeiziges Unterfangen, zügig gemeinsame Rechtsprechungsstandards zu entwickeln. Doch dadurch könne das gegenseitige Verständnis verbessert werden, um die aus Rechtsunsicherheit entstehenden Kosten und Handelsbarrieren zu senken.

Das kommende Thema: Big Data

Massendaten (»Big Data«) können Aufschluss über Entwicklungen der Zukunft geben, erläutern **Kenneth Neil Cukier** und **Viktor Mayer-Schoenberger** in *Foreign Affairs*. Big Data bezeichnet die Idee, durch die heute relativ kostengünstigen und leistungsstarken Computer riesige Datenmengen zu verarbeiten und daraus wahrscheinlichkeitsbasierte Hinweise auf Zusammenhänge zu erhalten. Die Masse der Daten sei dabei der ausschlaggebende Faktor. Waren bei früheren statistischen Analysen hochwertige Daten notwendig,

könnten bei Big-Data-Anwendungen variierende Datenqualitäten durch die enorme Menge von Daten ausgeglichen werden. Hinzu kommt, dass inzwischen fast alles in Daten abgebildet werden könne, etwa Ortsangaben in GPS-Daten. Was bei Big Data allerdings in den Hintergrund rücke, seien Ursache-Wirkungs-Zusammenhänge. Lediglich wahrscheinlichkeitsbasierte Aussagen seien möglich, aber diese könnten nach Ansicht der Autoren zur Lösung zahlreicher Probleme der Menschheit beitragen. Cukier und Mayer-Schoenberger präsentieren anschauliche Beispiele für eine sinnvolle Verwendung von Big Data, etwa in der Medizin oder in der Bereitstellung öffentlicher Dienstleistungen. Massendaten seien auch zur Bekämpfung des Klimawandels hilfreich. Eine Vielzahl von überall auf der Welt platzierten Sensoren könne einen Datenreichtum liefern, der es gestatte, die globale Erwärmung genauer zu bestimmen und die effizientesten Handlungsmöglichkeiten auszuloten. Immense Datenmengen vor allem in den Händen nichtdemokratischer Staaten könnten aber auch, so die Autoren, die Kluft zwischen Staat und Bürgern vergrößern, aus Big Data könne Big Brother werden.

Cybersicherheit als politische Herausforderung mit vielen Dimensionen

Die hier diskutierten Beiträge zeigen, dass die digitale Revolution nicht nur Chancen eröffnet, sondern auch erhebliche Risiken birgt. Das Wettrüsten der Nationen im Internet hat längst begonnen. Zudem ist durch Edward Snowdens Insider-Informationen über britische und amerikanische Überwachungsprogramme die enorme Bedeutung von Big Data für die Außen- und Sicherheitspolitik ins öffentliche Bewusstsein gelangt. »Man muss den Feind kennen, um ihn schlagen zu können« – dieser Grundsatz, den der chinesische Militärstratege Sunzi vor rund 2500 Jahren formulierte, hat gerade im Internet-Zeitalter seine Berechtigung. Wirkungsvolle IT-Sicherheitsmaßnahmen können nur dann getroffen werden, wenn bekannt ist, welche Methoden und Mittel der Gegner anwendet, um Rechner seines Kontrahenten zu hacken.

Gleichzeitig ist festzustellen, dass die digitale Revolution überaus unterschiedlich verläuft. So existiert eine digitale Kluft (digital divide) zwischen der OECD- und der Nicht-OECD-Welt. Das heißt, dass die Chancen auf den weltweiten Zugang zum Internet und zu anderen (digitalen) Informations- und Kommunikationstechniken ungleich verteilt sind und stark von sozialen Faktoren abhängen. Cybersicherheit erhält in diesem Sinne eine weitere Dimension, die der menschlichen Sicherheit. Offen ist die Frage, ob Aufrüstung und Abschreckung mehr Cybersicherheit schaffen werden oder ob sich eine neue Diplomatie, die sich auf die digitale Revolution einlässt, als nachhaltig erweisen wird. Aus den hier besprochenen Beiträgen wird klar, dass diese Diskussion erst begonnen hat. Die in den Artikeln behandelten Aspekte verdeutlichen, dass Cybersicherheit in zahlreichen Politikfeldern eine Rolle spielt und dass die informationstechnischen Möglichkeiten das Policy-making nachdrücklich verändern können. Daher stellt Cybersicherheit europäische und internationale Außen- und Sicherheitspolitik vor neue Herausforderungen.

Besprochene Aufsätze

Bamford, James, »The Secret War. Infiltration. Sabotage. Mayhem. For Years, Four-Star General Keith Alexander Has Been Building A Secret Army Capable of Launching Devastating Cyberattacks«, in: *Wired*, 12.6.2013

Bennett, Steven C., »The ›Right to Be Forgotten‹: Reconciling EU and US Perspectives«, in: *Berkeley Journal of International Law*, 30 (2012) 1, S. 161–195

Cilluffo, Frank J. / Sharon L. Cardash / George C. Salmoiraghi, »A Blueprint for Cyber Deterrence: Building Stability through Strength«, in: *Military and Strategic Affairs*, 4 (2012) 3, S. 3–23

Cukier, Kenneth Neil / Viktor Mayer-Schoenberger, »The Rise of Big Data«, in: *Foreign Affairs*, 1.5.2013, <www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data>

Cull, Nicholas J., »The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy«, in: *International Studies Review*, 15 (2013) 1, S. 123–139

Deibert, Ronald J. / Masashi Crete-Nishihata, »Global Governance and the Spread of Cyberspace Controls«, in: *Global Governance*, 18 (2012), S. 339–361

Dunn Cavelty, Myriam, »From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse«, in: *International Studies Review*, 15 (2013) 1, S. 105–122

Ebert, Hannes / Tim Maurer, »Contested Cyberspace and Rising Powers«, in: *Third World Quarterly*, 34 (2013) 6, S. 1054–1074 (im Erscheinen)

Lewis, James A., »In Defense of Stuxnet«, in: *Military and Strategic Affairs*, 4 (2012) 3, S. 65–76

Lindstrom, Gustav, »Meeting the Cyber Security Challenge«, Genf: Geneva Centre for Security Policy, Juni 2012 (GCSP Geneva Papers – Research Series, Nr. 7), <http://gcsp.ch/Regional-Capacity-Development/Euro-Atlantic-Security/Publications/GCSP-Publications/Geneva-Papers/Research-Series/Meeting-the-Cyber-Security-Challenge>

Schaake, Marietje, »Digital Freedom and Security in a Globally Connected World: Lessons from the MENA Region«, in: *Security and Human Rights*, 23 (2012) 3, S. 249–254

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 1611-6380