merics
Mercator Institute for China Studies

China Monitor

Nummer 19 | 8. Oktober 2014

Chinas *Cyber Security* (I): Divergenzen hinsichtlich Informationskontrolle, Sicherheitsstandards und Industriepolitik als Herausforderungen für das deutsche China-Engagement

von Hauke Johannes Gierow

ZENTRALE BEFUNDE UND SCHLUSSFOLGERUNGEN

- Deutschland und China haben ein vollkommen unterschiedliches Verständnis von *Cyber Security*. Während für Berlin die Sicherheit der Informationsnetze im Vordergrund steht, zielt Beijing auf eine umfassende Kontrolle der Informationen im Netz.

- Private IT-Firmen haben in China kaum Einfluss auf die Netzregulierung. Die chinesische Führung kann das Internet daher sehr viel umfassender regulieren als westliche Regierungen.

- Beijing betreibt eine aktive Industriepolitik im IT-Bereich, um eine international wettbewerbsfähige IT-Industrie zu entwickeln und von den USA unabhängig zu werden.

- Viele chinesische IT-Anbieter nutzen etablierte Sicherheitsstandards wie SSL *nicht* und verwenden stattdessen chinesische Alternativen. 2011 war rund jeder fünfte Internetnutzer in China von *Internetkriminalität* betroffen.

- China hat einen Überschuss an IT-Fachpersonal. IT-Experten, die keine adäquate Beschäftigung finden, werden häufig in der wachsenden IT-Schattenwirtschaft tätig und verstärken Sicherheitsrisiken im chinesischen Netz.

- Vernetzte Steuerungstechnik ist auch in China zunehmend Ziel von Hacker-Angriffen. 2010 infizierte der Stuxnet-Virus mehr als eintausend chinesische Firmennetzwerke und sechs Millionen PCs. Gravierende Sicherheitsrisiken sind für veraltete Steuerungssysteme in der chinesischen Infrastruktur (Staudämme, Kraftwerke etc.) zu identifizieren.

- China vertritt in internationalen Gremien der Netzregulierung ein extensives Verständnis von *Cyber Security* und staatlicher Informationskontrolle und nationaler Netzsouveränität. Die Durchsetzung universeller, international gültiger Transparenz- und Rechtsstandards wird durch die chinesischen Positionen gehemmt oder verhindert.

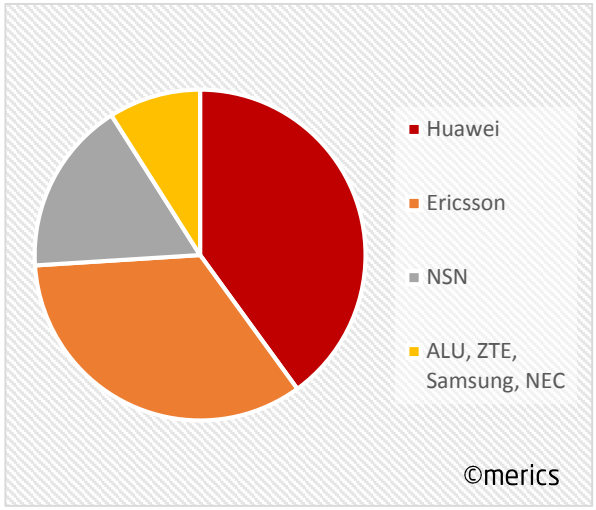
1 Warum Deutschland sich für chinesische *Cyber Security*-Politik interessieren sollte

„Made in China" ist eine auch in der IT-Branche weit verbreitete Produktkennzeichnung: 75 Prozent der weltweit verkauften Smartphones werden (nach chinesischen Angaben) in der Volksrepublik hergestellt. [1] Überraschender ist „Provided by China": **Die chinesischen Infrastrukturanbieter Huawei und ZTE haben direkten Einfluss auf die Kommunikation in Deutschland.**

Mobilfunk-Basisstationen von Huawei und ZTE sind in den schnellen Mobilfunknetzen aller deutschen Betreiber, die nach dem UMTS- bzw. dem LTE-Standard funken, vertreten. Übersicht 1 zeigt, dass Huawei etablierten Anbietern von Mobilfunklösungen insbesondere im schnellen LTE-Bereich Konkurrenz macht. [2]

Global vernetzte Produktions- und Entwicklungsabläufe erfordern eine verlässliche IT-Infrastruktur. Für Unternehmen ist *Cyber Security* ein entscheidender Standortfaktor für Investitionen. **Eine unsichere digitale Infrastruktur könnte langfristig das Investitionsklima in China verschlechtern.** [3]

Übersicht 1: Marktanteil LTE-Ausrüstungen 2013 (global), *Quelle: siehe Endnote 3*



Cyber Security ist nicht nur ein Thema für die IT-Wirtschaft: Moderne Industrieprodukte wie Anlagen im Maschinenbau enthalten Steuerungsanlagen und andere digital vernetzte Komponenten. Autohersteller müssen bei der Konzeption neuer Modelle die Software ebenso bedenken wie die Steuerung der Motorelektronik durch Mikroprozessoren.

Netzwerkgiganten wie Huawei oder ZTE versuchen, auch außerhalb Chinas Fuß zu fassen. Die Marktchancen sind jedoch in hohem Maße davon abhängig, wie viel Vertrauen den Unternehmen entgegengebracht wird. In den USA führte dieses mangelnde Vertrauen zu einem Beschluss des US-Kongresses: Huawei ist seit April 2013 von öffentlichen Aufträgen weitgehend ausgeschlossen.

In Deutschland ist Huawei mittlerweile auch mit Mobiltelefonen auf dem Markt für Privatkunden präsent. In Europa gewinnt die mobile Kommunikation seit Jahren an Bedeutung, verändert Lebenswelten aber nicht so radikal und umfassend wie in der Volksrepublik. Sicherheitslösungen für das mobile Internet stellen international eine große Herausforderung dar. China ist eine Pioniergesellschaft der digitalen Mobilität. Rund zwei Drittel der chinesischen Netizens nutzen das Internet via Smartphone oder Tablet. **Chinesische Lösungen im Bereich mobiler Sicherheit könnten deshalb Impulse für erfolgreiche *Cyber Security*-Politik für deutsche Politik und Unternehmen geben.** [4]

MERICS wird das Thema *Cyber Security* in einer Reihe von drei China-Monitoren behandeln. Diese erste Ausgabe gibt eine Einführung in das Thema. Der zweite Monitor wird sich mit den politischen Akteuren und Strategien beschäftigen, der dritte die Bedeutung von *Cyber Security* für die Wirtschaft in den Mittelpunkt stellen.

2 Zwischen Sicherheit und Kontrolle: *Cyber Security* ist ein umstrittenes Konzept

2.1 China, die USA und Europa reden aneinander vorbei

Grundlegende Begriffe der *Cyber Security* werden in westlichen Ländern anders definiert als in China oder Russland. In Europa und den USA ist der „*Cyberspace"* ein Begriff, der sowohl Technologien zur Übertragung von Informationen als auch gesellschaftliche Prozesse in der digitalen Sphäre umschreibt**. In Russland und China steht hingegen der *„Information Space"* im Mittelpunkt. Dieser Informationsraum umfasst auch die Kontrolle über Zeitungen, Publikationen oder sogar das menschliche Denken an sich und ist somit deutlich breiter definiert.**[5]

Diese unterschiedlichen Konzepte haben konkreten Einfluss auf internationale Verhandlungen: Bei Übersetzungen offizieller Dokumente gehen Feinheiten im Verständnis häufig verloren. Eine Vereinbarung kann daher im Nachhinein von allen Partnern sehr unterschiedlich umgesetzt werden.

Auch der Begriff *Cyber Security* selbst wird international unterschiedlich ausgelegt.

Die *International Telecommunications Union* (ITU), eine UN-Organisation, die vor allem für die Regulierung des Rundfunks und internationaler Funkfrequenzen zuständig ist, definiert *Cyber Security* wie folgt:

> *„Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. [...] Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."* [6]

Diese Definition ist sehr allgemein gehalten und an technischen Notwendigkeiten orientiert. Auch die Kriterien der ITU in Übersicht 2 ermöglichen unterschiedliche, länderspezifische Konkretisierungen. Die Ausgestaltung von *Cyber Security*-Politiken ist deshalb international sehr unterschiedlich.

Cyber Security bedeutet in Deutschland und Europa vor allem den Schutz kritischer Informationsinfrastrukturen, also der Datennetze selbst,

Übersicht 2: Kriterien für IT-Sicherheit

1. Die Verfügbarkeit von Informationsnetzen und -ressourcen (physisch vs. virtuell)
2. Die Integrität von Netzen und Informationen, also die Authentizität und Unanfechtbarkeit der Echtheit von Informationen (non-repudiation)
3. Die Geheimhaltung / Vertraulichkeit übermittelter Informationen.
4. Die Wirtschaftlichkeit sicherer IT-Systeme

der Stromversorgung, aber auch der administrativen Grundlagen. Maßgeblichen Einfluss hat das europäisch geprägte Konzept der „Zivilen Sicherheit". Infrastrukturanbieter und staatliche Behörden (z.B. das Innenministerium, das Bundesamt für Sicherheit in der Informationstechnik (BSI)) arbeiten eng zusammen. Die Bundeswehr spielt in Deutschland nur eine geringe Rolle für *Cyber Security*.

In den USA ist der Begriff weitaus stärker militärisch geprägt. Rüstungsanbieter haben ihr Produktportfolio in den vergangenen Jahren diversifiziert, um neue Geschäftsfelder zu erschließen. Private Unternehmen sehen ihre Geschäftsgeheimnisse zunehmend durch Spionage bedroht. Regierung und Unternehmer betrachten *Cyber Security* als eine der wichtigsten Voraussetzungen für den Bestand der nationalen Wettbewerbsfähigkeit.

Wichtige Unternehmen aus dem *Cyber Security-Bereich* pflegen enge Kontakte mit Entscheidungsträgern aus der US-Administration oder haben selbst lange Zeit in Ministerien gearbeitet. Wissenschaftler sprechen daher von einem Cyber-Industriellen-Komplex in den USA. Notwendige Entscheidungen werden dadurch behindert.[7]

Entscheidungsträger in den USA befinden sich in einem Zielkonflikt zwischen Wirtschaftsförderung und einem tatsächlichen Ausbau der Internetsicherheit, die sich nachteilig auf die eigene IT- und Rüstungswirtschaft auswirken könnte. Die Regierungen in Washington und London weisen einen großen Teil der *Cyber Security*-Budgets den Nachrichtendiensten bzw. dem Militär und den Geheimdiensten ihres Landes zu.[8]

Cyber Security verfolgt in China ähnliche Ziele wie in Deutschland und den USA: Es geht um leistungsfähige, widerstandsfähige Datennetze, den Schutz kritischer Infrastrukturen und sichere industrielle Steuerungsanlagen (Supervisory Control and Data Acquisition, SCADA).[9] Dem chinesischen Verständnis des „Information Space“ entsprechend hat die *Cyber Security*-Politik aber noch eine weitere Facette: In einer Rede auf dem China-UK Internet Roundtable 2013 forderte Lu Wei, Vize Propagandachef der Kommunistischen Partei Chinas und Chef des Nationalen Internetinformationsbüros (国家互联网信息办公室):

> *“Firstly, we call for an order of mutual respect. In the United Kingdom, being a "gentleman" means keeping to etiquette and order. In China, we have a parallel title junzi. Being a "junzi" means "not imposing on others what you yourself do not desire." We also need "Internet junzi" and "Internet gentlemen."* [10]

Partei und Regierung gehen in China gezielt gegen die Verbreitung von „Gerüchten” und „Falschinformationen” im Internet vor. Bis dato hat die chinesische Regierung jedoch keine genaue Definition für „Gerüchte“ vorgelegt. So können die zuständigen Behörden nahezu beliebig Informationen zu „Gerüchten“ erklären (s. MERICS-China Monitor 1). Konsequent betrachtet, spiegelt die vorherrschende Internetzensur das *Cyber Security*-Verständnis der chinesischen Führung wider: ***Cyber Security* bedeutet im chinesischen Kontext neben den genannten Kriterien der Informationssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Wirtschaftlichkeit) auch die Kontrolle über Informationen, die über das Netz verbreitet werden.**

Übersicht 3: Cyber Security im Vergleich (eigene Darstellung)

©merics	USA	China	Deutschland
Prägendes Kriterium	*Cyberwar*	Informationskontrolle	Zivile Sicherheit
Dominante Institution	Verteidigungsministerium, NSA, United States Cyber Command (USCYBERCOM)	Ministerium für Öffentliche Sicherheit, Volksbefreiungsarmee, Büro für Staatsgeheimnisse	Innenministerium, BSI, Katastrophenschutz
Interessen	Wirtschaftliche und politische Vormachtstellung verteidigen	umfassende Informationskontrolle	Schutz der Bevölkerung, Sicherung von Geschäftsgeheimnissen

Staats- und Parteichef Xi Jinping hat das Thema Internetsicherheit zu einem seiner Schwerpunkte erklärt. In einer neuen Führungsgruppe des Zentralkomitees der Kommunistischen Partei zur Internetsicherheit sollen alle Kräfte für eine *Cyber Security*-Politik gebündelt werden. Die neue Führungsgruppe ist Xi Jinping persönlich unterstellt. (Mehr zu diesem Thema in Teil 2 der Monitor-Serie zu *Cyber Security*).[11]

3 Herausforderungen für die chinesische *Cyber Security*-Politik

3.1 Entwicklung einer *Cyber*-Strategie

Weltweit dominieren private Akteure wie DENIC[12], ICANN[13] und IANA[14] die Internetregulierung. Der staatliche Einfluss auf wesentliche Gremien der Internetregulierung ist bis heute beschränkt. Im Gegenteil – das US-Handelsministerium gab im März 2014 bekannt, seine Kontrolle über die Internetverwaltung IANA abzugeben und auf eine internationale Multi-Stakeholder Plattform zu verlagern. Auch beim internationalen Verwaltungsgremium ICANN haben Regierungen nur einen Beobachterstatus und keine Veto-Macht.

In China regulieren hauptsächlich staatliche bzw. quasi-staatliche Akteuren das Internet: Die Kontrolle der Domainvergabe (.cn bzw. 中国) obliegt dem Nationalen Internetinformationsbüro und dem Ministerium für Industrie und Informationstechnologie (MIIT, 中华人民共和国工业和信息化部). Auch weitere Aufgaben der Netzregulierung (wie die Vergabe von SSL-Zertifikaten), die in westlichen Ländern durch zivilgesellschaftliche oder wirtschaftliche Initiativen wahrgenommen werden, obliegen in China staatlichen bzw. quasi-staatlichen Institutionen.[15]

Die chinesische Regierung schreibt dem Ausbau eigener IT-Kompetenzen eine große Bedeutung zu. **Anders als in westlichen Ländern ist der private Cyber-Sicherheitssektor weniger stark entwickelt und weniger einflussreich. Dies erweitert den Spielraum der chinesischen Administration:** Während Politiker in den USA bei ihren Planungen auf wirtschaftliche Interessen großer und mächtiger Player wie Boeing, General Dynamic und Raytheon Rücksicht nehmen müssen („regulatory capture"), ist dies in China bislang nicht der Fall.

Im Unterschied zu anderen Regierungen sieht die Führung in Beijing in der Dominanz amerikanischer Hard- und Software im IKT-Sektor eine Bedrohung der nationalen Sicherheit. Das Multi-Level-Protection Scheme (mehr dazu im zweiten Teil der Monitor-Reihe) verbietet den Einsatz von Windows 8 auf Behördencomputern.[16] Auch Privatnutzern wird von der Regierung nahegelegt, auf chinesische Linux-Versionen umzusteigen.[17] **Die Regierung hat realisiert, dass Kontrolle über IT-Systeme nur erreicht werden kann, wenn der Quellcode von Programmen offen zugänglich ist oder streng kontrolliert wird.**

Die weitere Entwicklung von IT-Sicherheitstechniken in China birgt laut Marktbeobachtern großes Wachstumspotential – bis 2017 soll der Markt sich auf knapp zehn Mrd. USD Umsatz verdoppeln.[18]

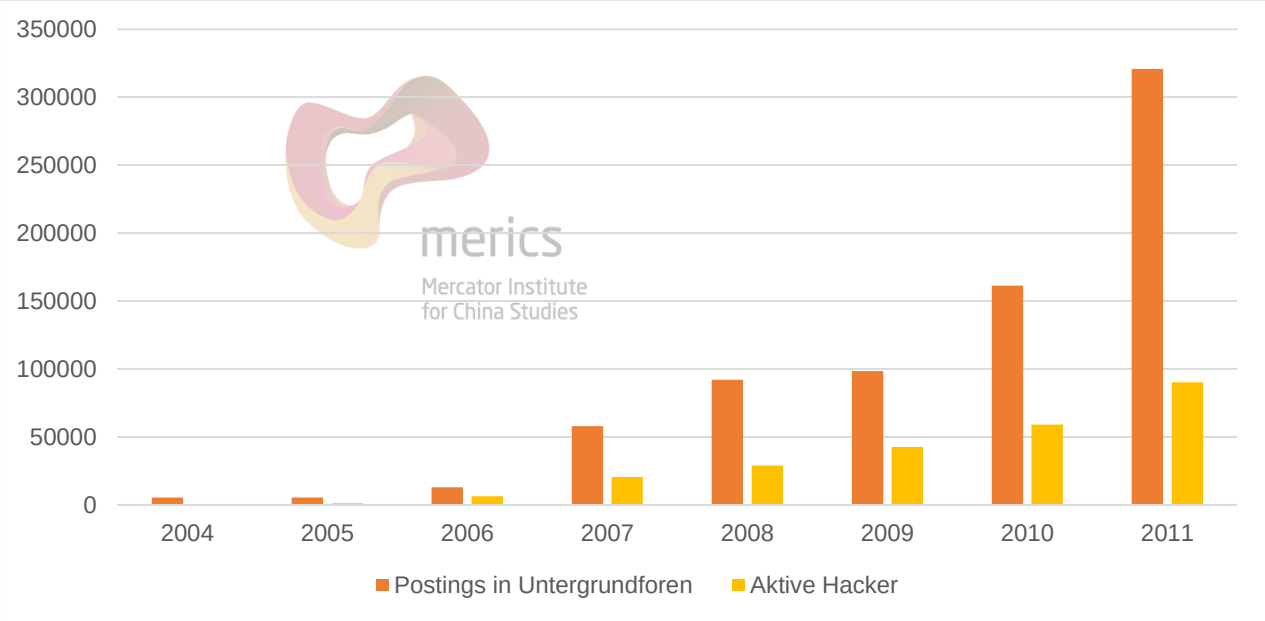
3.2 Sicherheit als Voraussetzung für Wirtschaftswachstum

China will seine Wirtschaft diversifizieren und dabei vor allem digitalisieren. Dafür ist Internetsicherheit für Nutzer und Firmen von besonderer Bedeutung.

Die zunehmenden Umsätze und die Dynamik des *E-Commerce* in China (siehe dazu MERICS China Monitor Nr. 15) machen Anbieter wie das chinesische Portal Taobao von Alibaba zu einem bevorzugten Angriffsziel. Banken und die mit Taobao und anderen Online Shopping-Plattformen verbundenen Zahlungsdienste wie Alipay sind aus diesem Grund besonders häufig Ziel von Phishing-Attacken. Bei dieser Form des Angriffs versuchen Hacker, mittels gefälschter E-Mails oder fingierter Login-Seiten Nutzerdaten abzugreifen.

Laut einer Analyse der Sicherheit von Online-Banking-Angeboten durch das staatliche chinesische Testcenter für Software (中国软件评测中心) kamen chinesische Banken im Schnitt nur auf ca. 30 von 100 möglichen Punkten.[19] Offizielle Dokumente zeigen ein dualistisches Verständnis von *Cyber Security*-Politik: **Einerseits fördert die Regierung durch Industriepolitik gezielt den Aufbau einer chinesischen IT-Industrie, die auch weltweit wettbewerbsfähig sein soll**. Dabei steht nicht nur Sicherheit im Fokus, sondern die Entwicklung neuer Geschäftsmodelle, qualifizierter Arbeitsplätze und innovativer Technologien. **Andererseits fördert Beijing gezielt auch nationale Sicherheitstechnologien und technische Standards. Diese sind im wachsenden *E-Commerce* von besonderer Bedeutung:** Viele chinesische Anbieter setzen verschlüsselte SSL-Verbindungen und andere etablierte Sicherheitsstandards noch nicht flächendeckend ein.[20]

Übersicht 4: Nachrichten in Untergrundforen und Anzahl aktiver Hacker, *Quelle siehe Endnote 20*



3.3 Arbeitslose IT-Spezialisten als Sicherheitsrisiko

In China gibt es einen Überschuss an IT-Fachpersonal. Viele Ingenieure und IT-Spezialisten schließen jedes Jahr ihr Studium ab.

Die Herausforderung für die chinesische Regierung ist trotzdem groß: **Wenn Absolventen keine für sie attraktive, legale Beschäftigungsmöglichkeiten finden, können sie unter Umständen Teil der IT-Untergrundökonomie werden**. Damit sind sie eine Gefahr für die Sicherheit der Netze und chinesische Internetnutzer. Übersicht 4 (siehe Seite 6) zeigt die rasante Zunahme von Teilnehmern in Untergrund-Hackingforen und die damit verbundenen Aufträge und Angebote krimineller Dienstleistungen.[21]

Ein Mangel besteht hingegen an qualifizierten Kräften, die Erfahrungen in internationalen Beziehungen und Policy-Expertise mitbringen und die an der Umsetzung von *Cyber Security*-Politik und der Umsetzung von Standards mitwirken können.[22]

3.4 Industrielle Steuerungsanlagen als Ziel von Cyber-Angriffen

Der im Jahr 2010 bekannt gewordenen Stuxnet-Angriff auf das iranische Nuklearprogramm machte deutlich, was Experten schon lange befürchteten: Industrielle Steuerungsanlagen sind verwundbar, und zunehmend Ziel von Cyber-Angriffen.

Das Stuxnet-Virus verbreitete sich weit über das eigentliche Angriffsziel Iran hinaus: **Auch China war von den Stuxnet-Angriffen betroffen: Nach Angaben der staatlichen Nachrichtenagentur Xinhua drang das Virus in mehr als sechs Millionen PCs und mehr als 1.000 Firmennetze ein**.[23] Illegale und veraltete Kopien von Software begünstigten die Verbreitung des Virus.

Ein potenzielles Ziel für Cyber-Angriffe stellen die in China weit verbreiteten Staudämme dar, allen voran der Drei-Schluchten-Staudamm am Yangtse-Fluss in Zentralchina. Deren Anlagen werden von vernetzten Computerchips gesteuert. Eine Manipulation birgt nach Meinung von Experten große Sicherheitsrisiken.[24] Im Ernstfall könnte es zum Überlaufen oder Bersten eines Dammes kommen. Oder aber massenhaft Wasser könnten abgelassen und so große Überflutungen ausgelöst werden. Nach Schätzungen von Experten wären davon rund 75 Mio. Menschen direkt betroffen.[25] Auch Angriffe auf Chinas Atomkraftwerke hätten katastrophale Folgen, da die Meiler oft in dicht besiedelten Gebieten stehen (u.a. in der Provinz Guangdong).

4 Chinas wachsender Einfluss auf internationale Netzregulierung

Das Stuxnet-Beispiel zeigt, dass Sicherheitsrisiken im Internet nicht isoliert in einem nationalen Kontext betrachtet werden können. Die unsichere IT-Infrastruktur eines Landes oder einer global agierenden Firma hat, insbesondere im Zeitalter von Cloud-Diensten, weitreichende Folgen für andere Regionen.

Westliche Industriegesellschaften haben sich daran gewöhnt, dass Produkte der Unterhaltungsindustrie in großem Maße in China hergestellt werden. Neu ist: Nicht nur die Produktion, sondern auch die Entwicklung vieler Technologien findet in China und durch chinesische Unternehmen statt.

Zwar berücksichtigen chinesische Unternehmen westliche Standards bei der Entwicklung, doch forciert die chinesische Regierung die Entwicklung eigener Technologien und Normen.

Auch in Fragen der internationalen Cyber-Zusammenarbeit agiert China zunehmend selbstbewusster und aktiver.

Gemeinsam bringen Russland und China seit Jahren alternative Resolutionen und Vorschläge in internationale Gremien wie die Vereinten Nationen ein, um die Internetregulierung zu verändern und eine stärkere Kontrolle durch Nationalstaaten zu ermöglichen.

Bislang konnten sich Schwellenländer mit den USA und Europa noch nicht auf eine einheitliche Plattform zur Beilegung ihrer Konflikte einigen: Während Europa und die USA auf das *Multi Stakeholder Internet Governance Forum* setzen, versuchen China, Russland und weitere autoritär regierte Staaten seit Jahren, der ITU *(International Telecommunications Union)* mehr Kompetenzen in der Netzregulierung einzuräumen. Bei der ITU Plenarsitzung 2012 in Dubai unterstützte eine Mehrheit der Mitglieder der ITU, unter ihnen China und Russland, einen entsprechenden Antrag. Westliche Industrieländer erkennen das neue Mandat der ITU bis heute nicht an.

Konflikte um die internationale Netzregulierung werden zunehmen. Deutschland, Europa und die USA sollten nach neuen Wegen der Kooperation mit chinesischen Akteuren suchen, wenn sie eine weitere Zersplitterung der Netzregulierung verhindern wollen. Diese hätte ähnliche Auswirkungen auf die Weltwirtschaft wie Protektionismus in der „analogen“ Wirtschaft. Die Verteidigung oder Verbreitung von aus westlicher Sicht unabdingbaren Rechts- und Transparenzstandards, die Informationsfreiheit und Privatsphäre schützen sollen, würde erschwert oder gar unmöglich.

Ansprechpartner für diesen China Monitor:
Hauke Gierow
Hauke.Gierow@merics.de

Impressum:
Mercator Institute for China Studies
Klosterstraße 64
10179 Berlin
Tel: +49 30 3440 999 – 0
Mail: info@merics.de
www.merics.org

[1] CRI Online (2014) Auch China hat nichts gegen Nokia-Übernahme durch Microsoft, http://german.cri.cn/3071/2014/04/10/1s214641.htm, Zugriff am 16.06.2014.
[2] Dyer, Keith (2013). Rising tide of LTE investment floating many boats: LTE vendor analysis. http://the-mobile-network.com/2013/09/rising-tide-of-lte-investment-floating-many-boats-lte-vendor-analysis/ Zugriff am 10.09.2014.
[3] Bloomberg News (2014).
Spying Charges Ratchet Up Fears for Multinationals in China. http://washpost.bloomberg.com/Story?docId=1376-N5VC806K50YT01-1TLGIC8M34KFP7U95A4VALELS2 Zugriff am 10.09.2014.
[4] Shu, Catherine (2014). China Now Has 700M Active Smartphone Users, Says Umeng, http://techcrunch.com/2014/03/13/china-now-has-700m-active-smartphone-users-says-umeng/ Zugriff am 09.07.2014.
[5] Giles, Keir und Hagestadt II, William (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and Englisch, http://www.ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf. Zugriff am 16.06.2014.
[6] International Telecommunications Union (Kein Datum). Definition of cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. Zugriff am 09.07.2014.
[7] Brito, Jerry und Watkins, Tate (2011). Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, http://mercatus.org/sites/default/files/WP1124_Loving_cyber_bomb.pdf Zugriff am 16.06.2014.
[8] Walker, Richard, W. (2014). Budget Bill Boosts Cybersecurity Spending,http://www.informationweek.com/government/cybersecurity/budget-bill-boosts-cybersecurity-spending/d/d-id/1113494. Zugriff am 18.07.2014.
[9] Staatsrat, 2012, „Policy Empfehlungen um die Entwicklung der Chinesischen Informationstechnologie und Informationssicherheit zu fördern“ (国务院出台意见推进信息化发展切实保障信息安全), http://politics.gmw.cn/2012-07/17/content_4571519.htm Zugriff am 14.08.2014, auch Segal, Adam (2012),China Moves Forward on Cybersecurity Policy http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/ Zugriff am 14.08.2014.
[10] Wei, Lu (2013). Liberty and Order in Cyberspace - Keynote speech at the Fifth China-UK Internet Roundtable. http://usa.chinadaily.com.cn/china/2013-09/09/content_16955871.htm. Zugriff am 09.07.2014.
11 Xinhuanet (2014). Xi Jinping leads Internet security group. http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm. Zugriff am 16.06.2014.
[12] DENIC ist eine genossenschaftliche Initiaitve der deutshcen Internetwirtschaft, die die Vergabe der Domains in Deutschland regelt.
[13] ICANN ist die Internet Corporation for Assigned Names and Numbers. Sie regelt die Verfahren zur Vergabe von IP-Adressen und *Top Level Domains* und ist eine zentrale Institution der *Internet Governance*.
[14] IANA – die Internet Assigned Numbers Authority- kümmert sich um die Verwaltung der DNS-Rootzone – einer Art Telefonbuch für das Internet. IANA ist zudem an der Verwaltung sogenannter generischer *Top Level Domains* beteiligt.
[15] Hachigian, Nina (2001) China’s Cyber-Strategy. Foreign Affairs. March / April 2001, http://www.foreignaffairs.com/print/56857. Zugriff am 14.08.2014.
[16] Kai, Jin (2014) Why China Banned Windows 8. http://thediplomat.com/2014/05/why-china-banned-windows-8/. Zugriff am 16.06.2014.
17 Chen, Stephen (2014). Chinese operating system? Still searching. South China Morning Post. http://www.scmp.com/news/china/article/1564503/chinese-operating-system-still-searching. Zugriff am 15.08.2014.
[18] AbiResearch (2013). $4.9 Billion Cyber Security Market in China Could Double by 2017 Despite Significant Foreign Barriers to Entry. https://www.abiresearch.com/press/49-billion-cyber-security-market-in-china-could-do. Zugriff am 05.09.2014.
[19] Goodrich, Jimmy (2012): Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy, S. 5f, in: Lindsay, John, China and Cybersecurity: Political, Economic, and Strategic Dimensions, http://igcc.ucsd.edu/assets/001/503568.pdf. Zugriff am 14.08.2014.
20 Segal, Adam (2012). China Moves Forward on Cybersecurity Policy. http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/. Zugriff am 16.06.2014.
[21] Zhuge Jianwei, Gu Liang und Duan Haixin (2012). Investigating China’s Online Underground Economy. http://igcc.ucsd.edu/assets/001/503677.pdf. Zugriff am 16.07.2014.
[22] Goodrich, Jimmy (2012): Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy, S. 5f., in: Lindsay, John, China and Cybersecurity: Political, Economic, and Strategic Dimensions, http://igcc.ucsd.edu/assets/001/503568.pdf (Zugriff am 14.08.2014).
[23] Xinhua (2010). Super virus hits 6 million computers in China, http://news.xinhuanet.com/english2010/china/2010-10/01/c_13538835.htm, Zugriff am 16.07.2014.
24 Adams, Patricia (2013). Cyberwar and secrecy threaten China’s dams, http://journal.probeinternational.org/2013/03/12/cyberwar-and-secrecy-threaten-chinas-dams/ Zugriff am 16.07.2014
[25] Philip B. Williams (1990). Dam Safety Analysis. In: Ryder, Grainne und Barber, Margaret (Hrsg.) Damming the Three Gorges: What Dam-Builders Don’t Want You To Know. Probe International. Auch Abrufbar unter: http://www.threegorgesprobe.org/pi/documents/three_gorges/damming3g/ch10.html. Zugriff am 20.09.2014.