merics
Mercator Institute for China Studies

China Monitor

Nummer 20 | 12. November 2014

Cyber Security in China (II): Neue politische Führung setzt auf Stärkung der nationalen Sicherheit

Neuordnung der Internet-Regulierung. Beschränkung ausländischer Software. Entwicklung eigener IT-Standards.

Von Hauke Johannes Gierow

ZENTRALE BEFUNDE UND SCHLUSSFOLGERUNGEN

- Chinas Staats- und Parteichef Xi Jinping hat *Cyber Security* zu einem Schwerpunkt der Regierungsarbeit gemacht. Wichtige Spitzenbeamte aus vielen Politikbereichen sind an der Ausarbeitung und Implementierung von *Cyber Security*-Politik beteiligt.

- China hat bislang keine kohärente *Cyber Security*-Strategie verfolgt. Die fehlende Bündelung von Entscheidungskompetenz führte zu einer uneinheitlichen Implementierung von *Cyber Security* und zu Machtkämpfen zwischen verschiedenen Ministerien.

- Der Nationale Arbeitsstab für Internet-Information wurde von Xi Jinping zum zentralen Akteur der *Cyber Security*-Politik aufgewertet. Lu Wei, der Leiter des Arbeitsstabes, positioniert sich zunehmend als Schlüsselakteur der Internet-Politik.

- Die chinesische Regierung betrachtet ausländische Software als potentielle Gefährdung für die nationale Sicherheit. Chinesische Unternehmen sind angehalten, einheimische Software zu benutzen, obwohl die zugelassenen chinesischen Alternativen häufig nicht so leistungsfähig und sicher sind wie westliche Angebote.

- Der Wunsch der chinesischen Regierung, die Sicherheit im Internet möglichst einheitlich und umfassend zu regulieren, kollidiert mit dem individuellen Sicherheitsbedürfnis der Internetnutzer. Sicherheitslücken in einheitlich vorgeschriebener Software können zu systemischen Einfallstoren für Hacker und Schadsoftware werden.

- Beijing gewinnt zunehmend größere Handlungsspielräume in der *Cyber Security*-Politik: Die Entwicklung eigener Sicherheitsstandards ist zwar kostspielig, China wird aber in der Tat immer unabhängiger von der ausländischen IT-Industrie.

1 „Ohne *Cyber Security* keine nationale Sicherheit."

„Ohne *Cyber Security* keine nationale Sicherheit" (没有网络安全就没有国家安全), sagte Staats- und Parteichef Xi Jinping im April 2014 gegenüber der staatlichen Nachrichtenagentur Xinhua.[1] Die aktuelle Führung in Beijing misst *Cyber Security* deutlich mehr Bedeutung bei als noch vor einigen Jahren. Zur Verbesserung der Cyber-Sicherheit greift die chinesische Regierung zunehmend zu protektionistischen Maßnahmen.

Software westlicher Hersteller wird von der chinesischen Regierung als Sicherheitsrisiko wahrgenommen. Ihr Einsatz in China ist daher streng reglementiert. Diese Regulierung lässt bereits erste internationale Auswirkungen erkennen. Die chinesische *Cyber Security*-Politik hat insgesamt das Potenzial, den globalen Markt für IT-Produkte und Dienstleistungen grundlegend zu verändern.

Chinas Regierung ergreift derzeit konkrete Schritte zur Erhöhung der Cyber-Sicherheit: Im Frühjahr 2014 hat sie die „Zentrale Führungsgruppe für Cyber-Sicherheit und Informatisierung" (中央网络安全和信息化领导小组) gegründet. Dass Staats- und Parteichef Xi Jinping die Führung dieser Gruppe übernommen hat, zeigt die Bedeutung des Themas für die chinesische Regierung. Unterstützt wird Xi von Ministerpräsident Li Keqiang, dem Leiter der ZK-Kanzlei der KPCh, Liu Yunshan, und dem Chef der chinesischen Zentralbank, Zhou Xiaochuan.[2]

2 *Cyber Security* als Führungsaufgabe

2.1 Grundlagen der Cyber Security-Politik

Das Thema Cyber-Sicherheit beschäftigt die Regierung in Beijing schon seit mehr als zehn Jahren: Bereits 2003 arbeitete die „Führungsgruppe zur Koordinierung der Netzwerk- und Informationssicherheit"（全国网络与信息安全协调小组） die erste chinesische *Cyber Security*-Strategie aus. Das sogenannte „Dokument 27" („Stellungnahme der nationalen Führungsgruppe für Informatisierung bezüglich der Verbesserung von Informationssicherheit"; 国家信息化领导小组关于加强信息安全保障工作的意见) legte den Grundstein für mehrere Politikentscheidungen, die bis heute prägend sind. Seit der Verabschiedung des Dokumentes 27 wurde die *Cyber Security*-Politik weiterentwickelt. Die aktuelle *Cyber Security*-Strategie stammt von 2012 („Stellungnahme des Staatsrats zur Förderung der Informatisierung und für den Schutz der Informationssicherheit"; 国务院关于大力推进信息化发展和切实保障信息安全的若干意见).[3]

Diese Strategie definiert ein relativ breites Spektrum an Zielen:

- Die Stärkung des Breitbandausbaus in China, insbesondere in ländlichen Regionen
- Die Entwicklung chinesischer Sicherheitstechnologien
- Die verstärkte Kontrolle des Netzes, um die „Aufrechterhaltung guter Sitten im Netz" sicherzustellen
- Die Erforschung mobiler Netzwerke der nächsten Generation (5G)
- Den Ausbau von *E-Government*-Dienstleistungen in China. [4]

Für die Gewährleistung von *Cyber Security* sollen zudem kritische Infrastrukturen geschützt und chinesische Kryptographie-Standards entwickelt werden.[5]

2.2 Machtkämpfe um Cyber Security

Die ständig wechselnden Zuständigkeiten und die Auflösung der ersten Führungsgruppe im Jahr 2008 hatte in den vergangenen Jahren eine mangelnde Bündelung der Entscheidungs-kompetenzen zur Folge. **Einige Ministerien haben ver-**

sucht, diesen Freiraum zu besetzen, um ihre eigene Rolle im wichtiger werdenden Feld der Netzregulierung zu sichern. Von politischer Seite vorgegebene Maßnahmen wurden nicht konsequent umgesetzt, da einzelne Ministerien ihre eigenen Interessen in den Vordergrund stellten. [6]

Bis heute bestehen zum Beispiel unterschiedliche Sicherheitsstandards verschiedener Ministerien nebeneinander. Firmen, die ihre Technologie an diese Ministerien verkaufen wollen, müssen sich jeweils einer aufwändigen Zertifizierung unterziehen und ihre Software gegebenenfalls anpassen. Insbesondere kleine IT-Startups können das nicht leisten – viele von Ihnen verzichten daher zurzeit auf den eigentlich lukrativen Markt des öffentlichen Sektors. Dies hemmt die Entwicklung einer starken chinesischen IT-Wirtschaft.

Auseinandersetzungen gibt es jedoch nicht nur um Zuständigkeiten, sondern auch um die Frage, wie weit die Zensur des Internets gehen sollte. Nach Ansicht verschiedener Entscheidungsträger und lokaler Beamter behindert eine strenge Kontrolle die wirtschaftliche Entwicklung Chinas. Über das „richtige Maß“ herrscht innerhalb der Regierung Uneinigkeit.

Deutlich wird dieser Konflikt am Beispiel neuer Freihandelszonen. Presseberichten aus Hongkong zufolge sollte in der Freihandelszone in Shanghai ursprünglich auf Internetzensur vollständig verzichtet werden. Spitzenbeamte dementierten diese Aussage später jedoch gegenüber staatlichen Medien. Lokale Entscheidungsträger aus Shenzhen kündigten wiederum an, dass die Freihandelszone Qianhai auf Internetzensur verzichten werde.[7]

2.3 Priorisierung von Cyber Security unter Xi

Mehrere politische Akteure arbeiten an der Ausarbeitung der *Cyber Security*-Politik. Die 2014 von Staats- und Parteichef Xi Jinping berufene „Zentrale Führungsgruppe für Cyber-Sicherheit und Informatisierung“ bringt hochrangige Spitzenbeamte mit Vertretern verschiedenster Ministerien zusammen (unter anderem aus dem Finanz-, Bildungs- und Kulturministerium sowie der Nationalen Reform- und Entwicklungskommission).

Die Führungsgruppe ist kein Exekutivorgan, sondern erarbeitet vor allem Leitlinien für die *Cyber Security*-Politik. Einige Mitglieder sind bewusst in gleich mehreren, nebeneinander bestehenden Gruppen wie der „Zentralen Führungsgruppe zur umfassenden Vertiefung der Reformen “ （中央全面深化改革领导小组， siehe MERICS China Monitor Nr. 13) präsent. Diese Verschränkung soll die Transparenz und Zusammenarbeit untereinander stärken.

Übersicht 1: Wegbereiter der *Cyber Security*-Politik

Eigene Darstellung: Hauke Gierow

Die enge Anbindung der Führungsgruppe an den Nationalen Arbeitsstab für Internet-Information (国家互联网信息办公室) soll zudem eine schnelle Umsetzung von Richtlinien und Gesetzen ermöglichen.[8]

Dessen Vorsitzender, Lu Wei, leitet auch den Arbeitsstab der Führungsgruppe und nimmt in der *Cyber Security*-Politik eine Koordinierungsfunktion ein. Unmittelbar nach dem 4. Plenum des Zentralkomitees der Kommunistischen Partei bestellte er

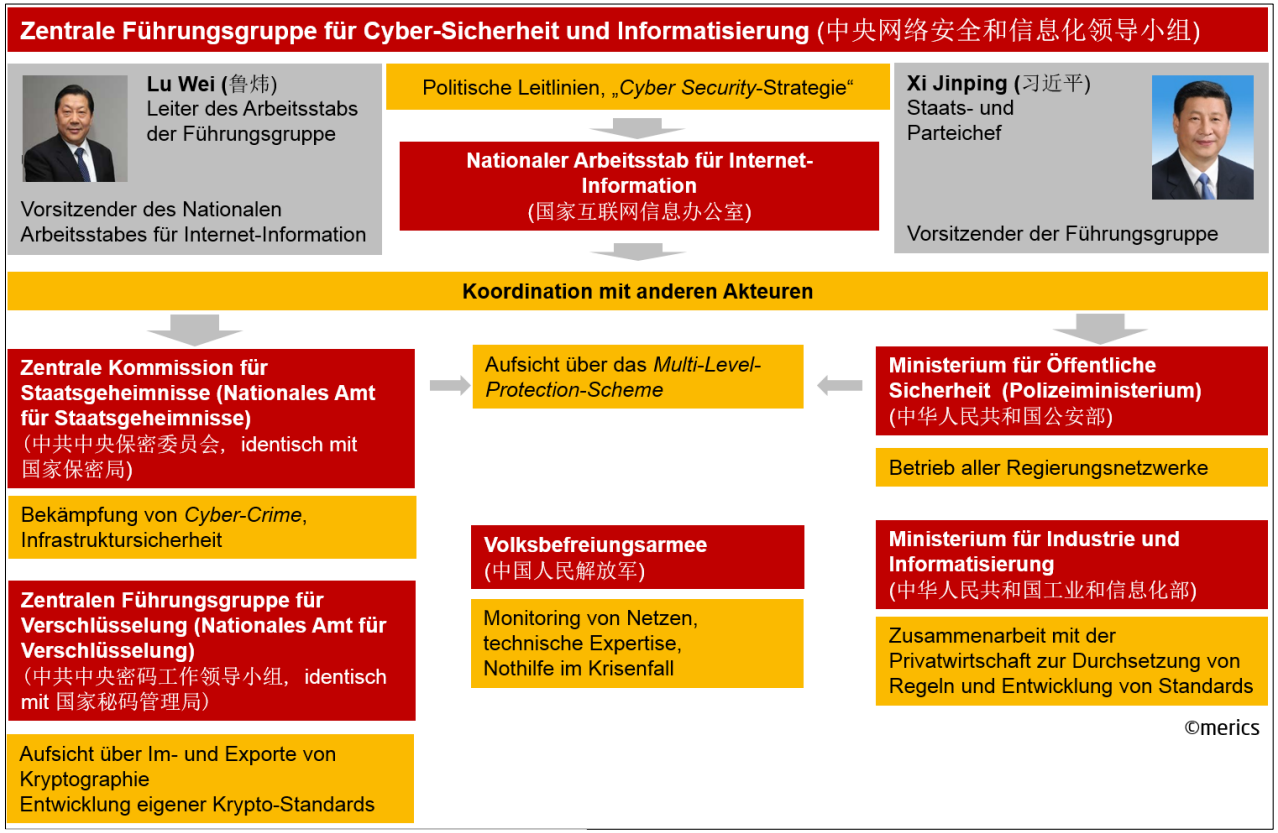
Vertreter lokaler Propagandabüros und Arbeitsstäbe für Internet-Information sowie von Firmen und Medien aus ganz China ein, um „Gespräche über die weitere Verrechtlichung des *Cyber-Space*“ (谈推进网络空间法治化) zu führen.[9] **Das Beispiel zeigt, dass der Nationale Arbeitsstab für Internet-Information durch Xi Jinping zum zentralen Akteur der *Cyber Security*-Politik aufgewertet wurde.**

Die hochkarätige Besetzung der neuen Führungsgruppe und die koordinierende Rolle des Nationalen Arbeitsstabes für Internet-Information entfalten Signalwirkung innerhalb des politischen Systems: Die chinesische Regierung hat die Bedeutung des Themas erkannt und will in den kommenden Jahren bestehende Defizite beheben. Auch die herausgehobene Stellung, die viele frühe Wegbereiter der *Cyber Security*-Politik heute im politischen System innehaben, eröffnet neue Gestaltungspielräume (siehe Übersicht 1).

2.4 Sicherheitssektor in der Verantwortung

Im Arbeitsalltag sind vor allem jene Ministerien für *Cyber Security*-Politik zuständig, die sich ohnehin mit sicherheitsrelevanten Fragen beschäftigen: Das Ministerium für Öffentliche Sicherheit (中华人民共和国公安部) verantwortet die Bereiche *Cyber-Crime*, Infrastruktursicherheit und – in

Übersicht 2: Zentrale Akteure der *Cyber Security*-Politik



Eigene Darstellung: Hauke Gierow / Lea Shih

Zusammenarbeit mit der Zentralen Kommission für Staatsgeheimnisse（中共中央保密委员会，identisch mit dem Nationalen Amt für Staatsgeheimnisse, 国家保密局) – das *Multi-Level-Protection-Scheme* (eigentlich *Regulations on Classified Protection of Information Security*, 信息安全等级保护管理办法, MLPS, nähere Analyse in Abschnitt 3).

Das Ministerium für Industrie und Informatisierung (中华人民共和国工业和信息化部）koordiniert die Zusammenarbeit mit der Privatwirtschaft. Die Generalstabsabteilung der Volksbefreiungsarmee (中国人民解放军总参谋部) stellt vor allem Informationen über Cyber-Angriffe bereit. Sie unterstützt die Zentrale Kommission für Staatsgeheimnisse beim Betrieb der geheimen Regierungsnetze. Eine detaillierte Darstellung der Akteure und ihrer Zuständigkeiten liefert Übersicht 2.

3 Sicherheitsbedenken oder Industriepolitik?

3.1 Das Multi-Level-Protection-Scheme (MLPS) *als Herzstück der Cyber Security-Politik*

Herzstück der aktuellen chinesischen *Cyber Security*-Politik ist die Entwicklung einer leistungsfähigen IT-Industrie im Land, um die potentielle Bedrohung durch ausländische Software zurückzudrängen. Das MLPS soll helfen, diese Gefahr abzuwehren.

Sicherheitskritische Bereiche, etwa Behörden oder strategisch wichtige Firmen, müssen verstärkt Technologien einsetzen, die von chinesischen Staatsbürgern beziehungsweise Firmen entwickelt wurden. **Dies soll verhindern, dass sich ausländische Regierungen über *Backdoors* Zugang zu geheimen Informationen verschaffen.** Die Kriterien dazu sind ursprünglich aus dem Zertifizierungsverfahren des 2003 veröffentlichten „Dokuments 27“ hervorgegangen. Während der vergangenen Jahre wurde ihre Anwendung immer weiter verstärkt.[10]

Das Ministerium für Öffentliche Sicherheit und die Behörde für den Schutz von Staatsgeheimnissen haben mit dem MLPS seit 2008 ein Verfahren entwickelt, das IT-Sicherheitsvorschriften in verschiedenen Sicherheitsstufen vorsieht. Sie gelten für:

- Privatanwender und kleine Firmen (Stufen 1+2),
- Unternehmen in strategisch wichtigen Sektoren (Finanzen, Infrastruktur und andere, Stufe 3)
- sowie Behörden (Stufen 4+5).

Eine Zusammenstellung der Kriterien liefert Übersicht 3.[11]

Übersicht 3: Kriterien des MLPS ab Stufe 3

Nr.	Kriterium für sicherheitsrelevante IT-Produkte
1	Die Produktentwicklung wurde von chinesischen Bürgern, juristischen Personen oder Firmen mit staatlicher Beteiligung durchgeführt
2	China hält das geistige Eigentum an Schlüsselkomponenten der Technologie.
3	Am Produktionsprozess beteiligte Personen haben keinerlei Vorstrafen.
4	In die Produkte wurden keine *Backdoors* oder Trojaner eingebaut.
5	Die Produkte stellen keine Gefahr für die nationale Sicherheit, öffentliche Ordnung oder öffentliche Interessen dar.
6	Die Software ist für Erfordernisse der nationalen Sicherheit zertifiziert.

©merics

Die Vorschriften haben bereits jetzt **drastische Auswirkungen auf westliche Unternehmen**: Microsoft kann sein Windows-Betriebssystem nicht mehr an chinesische Behörden verkaufen, und Hersteller von Antivirus-Software wie Kaspersky oder Symantec haben keinen Zugang mehr zu Unternehmen, die der Sicherheitsstufe 3 zugeordnet sind.

Auch Deutschland verfügt über detaillierte Regelungen für sichere IT-Produkte. Öffentliche IT-Aufträge werden nur an Unternehmen vergeben, die die sogenannten IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einhalten. International gibt es mit den *Common Criteria* ähnliche Regelungen. [12]

Von den bestehenden internationalen Vereinbarungen grenzt sich China jedoch bewusst ab: Beijing investiert stattdessen in die Entwicklung von IT-Parallelstandards wie die W-Lan-Verschlüsselung WAPI und die alternative Mobilfunktechnik TD-SCDMA.

Gleichzeitig wendet China die definierten Sicherheitskriterien viel breiter an, als westliche Industrieländer. Banken und andere wichtige Unternehmen müssen etwa auch in Deutschland und den USA Standards im IT-Bereich beachten. Die Vorschriften sind jedoch weniger detailliert und nicht so stark abgestuft. Auch gibt es bislang keinen Ausschluss eines kompletten Landes. Nicht nur in China, sondern auch in den USA sind jedoch protektionistische Tendenzen erkennbar.

Aus Sicht der chinesischen Regierung ist die Beschränkung ausländischer Software in sicherheitskritischen Bereichen nachvollziehbar: Gerade Betriebssysteme und Virenscanner sind potentielle Schwachstellen und können einen nahezu unbegrenzten Zugriff auf PCs und Serversysteme erlauben.

3.2 Internationale Konflikte um IT-Ausrüstung

Die USA werfen China seit Jahren vor, Industriespione staatlich zu unterstützen. Im Sommer 2014 verschärfte sich der Konflikt, als das amerikanische Justizministerium fünf angebliche IT-Spione aus China anklagte. Die Führung in Beijing reagierte empört und bezeichnete die Vorwürfe als konstruiert.[13]

Dabei spielten der chinesischen Regierung auch die durch Enthüllungen des US-Whistleblowers

Übersicht 4: *Multi-Level-Protection-Scheme*

Stufe	Betroffene	Folgen bei Ausfall der IT	Sicherheits-anforderungen	Betroffene ausl. Software (Beispiel)
1 + 2	Privatanwender / kleine und mittlere Unternehmen	Individuelle Schäden, keine unmittelbare Gefahr für die Gesellschaft	Selbstschutz von Nutzern + Unternehmen etwa durch Firewall / Virenscanner	Keine Vorschriften
3	Unternehmen aus den Bereichen Energie, Finanzen, Transport, Infrastruktur	Gefahr für die soziale Ordnung und das öffentliche Interesse. Evtl. Schäden für die nationale Sicherheit.	Vorschriften für Zugang und Nutzung der Systeme, Information der Behörden über Tests und Sicherheitsrisiken. Jährliche Sicherheitsüberprüfung.	Ausländische Antivirus-Software wie Symantec oder Kaspersky, Business-Software
4	Behörden	Besonders schweren Schaden für öffentliche Interessen / Schwere Schäden für nationale Sicherheit.	Klar definierte Schutzniveaus und Zugriffsberechtigungen, erweiterte Sicherheitstests, „Trusted Computing" Hardware. Sicherheitsüberprüfung alle sechs Monate.	Windows-Betriebssystem + vorherige Stufen
5 ©merics	Behörden mit erhöhten Sicherheits-anforderungen	Besonders schwere Schäden für nationale Sicherheit.	Verpflichtende Zugangskontrolle, Minimale Komplexität der Systeme. Fortlaufende Sicherheitsprüfung.	Windows-Betriebssystem + vorherige Stufen

Eigene Darstellung: Hauke Gierow. Quelle: Vgl. Endnote 10.

Edward Snowden bekannt gewordenen Überwachungsmaßnahmen der NSA in die Hände. Denn sie offenbarten im vergangenen Jahr, dass die US-Regierung gezielt Schwachstellen auch in amerikanischen Hard- und Softwareprodukten nutzt, um Spionage zu betreiben. Medienberichten zufolge haben Mitarbeiter der NSA diese Schwachstellen sogar gezielt eingebaut, etwa bei Routern der Firma CISCO.

Von den Auseinandersetzungen profitierten chinesische IT-Unternehmen: Die Aktienkurse verschiedener Firmen wie Yonyou und Inspur stiegen 2014 deutlich an. Dies lag unter anderem daran, dass die chinesische Regierung als Reaktion auf das amerikanische Vorgehen verkündete, die Kriterien des MLPS strenger anzuwenden und den chinesischen IT-Markt weiter zu fördern.[14]

Auch die USA beschränken den Import chinesischer Software aus Sicherheitsgründen. Bereits 2013 unterzeichnete Präsident Obama ein Gesetz, das die Beschaffung chinesischer Technologie durch amerikanische Bundesbehörden verbietet. Auch privaten US-Unternehmen wird nahegelegt, auf chinesische Technik zu verzichten.

3.3 Regeln schaden Wettbewerbsfähigkeit

Die strengere Anwendung des MLPS stellt chinesische Firmen teilweise vor Probleme. Denn die Technologien aus dem eigenen Land bieten den Anwendern oft nicht den gleichen Komfort wie US-Produkte, teilweise fehlen ihnen sogar wichtige Funktionen.

Die chinesische Regierung nimmt die Nachteile für die Unternehmen und deren hohe Anpassungskosten in Kauf. Die Umstellung von IT-Systemen geschieht auch in China nicht über Nacht: Aktuell werden bei der China Postal Savings Bank probeweise Server von IBM durch Produkte der chinesischen Firma Inspur ersetzt. Diese Tests sollen mittelfristig auf weitere Geldhäuser ausgeweitet werden.[15]

4 Warum mehr Überwachung und Kontrolle nicht mehr Sicherheit bringt: Das Beispiel *Green Dam*

Mehr staatliche Kontrolle im Internet führt nicht zwingend zu mehr Sicherheit für die Bürger. Das hat die Einführung der Software *Green Dam* im Jahr 2009 gezeigt. Um den Jugendschutz im Netz zu stärken, wurde die Software seit 2008 im Auftrag des MIIT entwickelt. Sie sollte pornographische Inhalte automatisch blockieren. Nach einer Anweisung des MIIT mussten Firmen alle in der Volksrepublik verkauften PCs mit diesem Programm ausrüsten – Stichtag war der 1. Juli 2009. Auch auf PCs in deutschen Schulen sind vergleichbare Anwendungen installiert – jedoch nicht verpflichtend.

In China bemängelten Kritiker 2009, die Software verstärke die ohnehin strenge Internetzensur weiter. Denn *Green Dam* blockierte auch regierungskritische Webseiten. Chinesische IT-Sicherheitsexperten stellten zudem gravierende Sicherheitslücken fest, die aufgrund der erforderlichen Vorinstallation des Programms dazu führten, dass Hacker die Sicherheitslücken nutzen und alle so ausgerüsteten PCs ausspionieren konnten.

Sowohl *Netizens* als auch Unternehmen äußerten deswegen lautstarken Unmut über die verpflichtende Installation. Schließlich nahm die Regierung die Regelung nur wenige Monate nach Inkrafttreten wieder zurück. Die *Green Dam*-Herstellerfirmen sind mittlerweile insolvent.[16]

Das Beispiel zeigt: Die erzwungene Installation von einheitlicher Software kann ein akutes Sicherheitsproblem darstellen. Wenn alle Systeme die gleiche Software nutzen, sind sie im Falle von Mängeln

auch alle verwundbar. **Der Wunsch der chinesischen Regierung, die Sicherheit im Internet möglichst einheitlich und umfassend zu regulieren, kollidierte hier mit dem individuellen Sicherheitsbedürfnis der Internetnutzer.**

5 Schlussbetrachtung

Die chinesische Führung nutzt ihren Einfluss auf alle relevanten Institutionen der Netzregulierung, um weitgehende Projekte wie das MLPS zu realisieren. In den vergangenen Jahren fehlte es jedoch an politischer Führung, um die beschlossenen Maßnahmen auch durchzusetzen.

Die aktuelle Regierung hat dieses Defizit erkannt. Sie ergreift mit der neuen Führungsgruppe und der gestärkten Rolle des Nationalen Arbeitsstabes für Internet-Information konkrete Maßnahmen zur Verbesserung der Internetsicherheit.

In den vergangenen Jahren gab es jedoch nicht nur in China Schwierigkeiten bei der Umsetzung von *Cyber Security*-Politik. Auch in anderen Ländern gibt es Probleme – jedoch an anderer Stelle. In Deutschland zum Beispiel ist *Cyber Security* nach wie vor kein Schwerpunkt der Politik. Von der Bundesregierung beschlossene Maßnahmen wie die Einführung einer *No-Spy*-Klausel oder die Errichtung eines neuen, eigenen Kommunikationsnetzwerkes des Bundes werden von IT-Experten und Behörden wie dem Bundesrechnungshof als halbherzig und unwirksam bezeichnet.[17]

Auch in den USA gibt es seit Jahren kaum Bewegung in der *Cyber Security*-Politik. Wissenschaftler machen dafür unter anderem die enge Verknüpfung privater Unternehmen aus dem IT-Sicherheitsbereich mit Mitarbeitern der Administration verantwortlich.[18] Der Entscheidungsspielraum der US-Administration ist durch die Bedeutung des IT-Sektors begrenzt – die USA können die Sicherheit eigener Technologien nicht öffentlich in Frage stellen. Weil sie kein Gehör fanden, haben bereits mehrere Sonderbeauftragte für Internetsicherheit im Weißen Haus ihren Job aufgegeben.[19] Auch die Enthüllungen Edward Snowdens haben die Debatte über die Sicherheit amerikanischer Softwareprodukte beflügelt – und könnten der Wettbewerbsfähigkeit der US-IT-Wirtschaft langfristig schaden.

Chinas Aufbau einer eigenen IT-Industrie wird die bestehenden weltweiten Strukturen in den kommenden Jahren massiv verschieben. Die gezielte industriepolitische Förderung im IT-Bereich und der Export chinesischer Technologien in Partnerstaaten in Afrika und Asien haben das Potenzial, die bisherige Dominanz der USA in der IT-Industrie anzugreifen und einzuschränken.

Ausländische Unternehmen müssen daher mit wachsenden Barrieren auf dem chinesischen Software-Markt rechnen. Wenn der derzeit erkennbare Trend zur Verschärfung chinesischer Sicherheitsstandards anhält, wird das Geschäftsumfeld vor allem für US-amerikanische Anbieter noch schwieriger werden.

Einige Softwarehäuser aus Europa, wie zum Beispiel SAP, scheinen von dieser Kontrolle bislang nicht so stark betroffen zu sein – wohl auch, weil deren Produkte für viele chinesische Firmen derzeit noch unverzichtbar sind.

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] Xinhuawang 新华网 (2014). „习近平：把我国从网络大国建设成为网络强国“ (Xi Jinping: China muss von einer großen Internetnation zu einer mächtigen Internetnation werden), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm Zugriff: 28.09.2014.

[2] Xinhuanet (2014). „Xi Jinping leads Internet security group.” http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm. Zugriff: 16.06.2014.

[33] Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2012). „国务院出台意见推进信息化发展切实保障信息安全.”（Der Staatsrat formuliert Meinungen zur Förderung der Informatisierung und für den Schutz der Informationssicherheit), http://politics.gmw.cn/2012-07/17/content_4571519.htm Zugriff: 14.08.2014.

[4] Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2012). „国务院出台意见推进信息化发展切实保障信息安全.” (Stellungnahme des Staatsrats zur Förderung der Informatisierung und für den Schutz der Informationssicherheit), http://politics.gmw.cn/2012-07/17/content_4571519.htm Zugriff: 14.08.2014; Segal, Adam (2012). „China Moves Forward on Cybersecurity Policy” http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/ Zugriff: 14.08.2014.

[5] Zhonggongzhongyang bangongting 中共中央办公厅 (2003): „关于加强信息安全保障工作的意见.”（Meinung der Führungsgruppe zur Stärkung der Informationssicherheit), http://www.360doc.com/content/14/0423/10/93013_371341672.shtml. Zugriff: 14.08.2014.

[6] Goodrich, Jimmy (2012). „Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy”, In: Lindsay, John (Ed.)(2012). China and Cybersecurity: Political, Economic, and Strategic Dimensions, 5-7. http://igcc.ucsd.edu/assets/001/503568.pdf. Zugriff: 14.08.2014.

[7] Luisetta Mudie (2013) „Party Paper Rules Out Internet Freedoms in Shanghai Free Trade Zone”, http://www.rfa.org/english/news/china/internet-09272013104820.html Zugriff:16.06.2014.

[8] China Copyright and Media (2014). „Cybersecurity and Informatization Leading Group: Names and Documents. “ http://chinacopyrightandmedia.wordpress.com/2014/03/13/cybersecurity-and-informatization-leading-group-names-and-documents/ Zugriff: 05.09.2014; Guancha zhe 观察者(2014). „中央网络安全和信息化领导小组成员名单 12 正副国级兼职深改组.” (Liste der Mitglieder der Zentralen Führungsgruppe zur Erhöhung der Internetsicherheit und Informatisierung: 12 Spitzenpolitiker der Staatsebene nehmen Teil) http://www.guancha.cn/politics/2014_02_28_209672.shtml. Zugriff: 05.09.2014

[9] Xinhuawang 新华网（2014). „全国网信办主任在京座谈推进网络空间法治化“ (Direktor des Nationalen Arbeitsstabes für Internet-Information in Beijing: Die Diskussion über die Verrechtlichung des Cyberspace voranbringen) http://news.xinhuanet.com/politics/2014-10/26/c_1112981005.htm Zugriff: 28.10.2014.

[10] Bischoff, Paul (2014) „Which Chinese tech companies benefit from *Cyber Security* row with US?”, http://www.techinasia.com/chinese-tech-companies-benefit-cyber-security-row/ Zugriff: 24.07.2014.

[11] Zhonghua renmin gongheguo gong'an bu 中华人民共和国公安部 (2007). „信息安全等级保护管理办法“(Maßnahmen zum Management der Stufen der Informationssicherheit), http://www.mps.gov.cn/n16/n1282/n3493/n3793/n494630/494907.html Zugriff: 05.09.2014.

[12] Die *Common Criteria*, vereinbart zwischen Kanada, Frankreich, Deutschland, Großbritannien und den Vereinigten Staaten, Australien, Neuseeland, Japan und Spanien, siehe dazu: Ernst, Dieter und Martin, Sheri (2010). „The Common Criteria for Information Technology Security Evaluation — Implications for China's Policy on Information Security Standards.” http://www.eastwestcenter.org/fileadmin/stored/pdfs/econwp108.pdf Zugriff: 14.08.2014.

[13] Williams, Pete (2014). “U.S. Charges China With Cyber-Spying on American Firms.” http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706 Zugriff: 26.08.2014.

[14] Bischoff, Paul (2014) „Which Chinese tech companies benefit from *Cyber Security* row with US?”, http://www.techinasia.com/chinese-tech-companies-benefit-cyber-security-row/ Zugriff: 24.07.2014.

[15] Yang, Steven (2014). „China Said to Study IBM Servers for Bank Security Risks.” http://www.bloomberg.com/news/2014-05-27/china-said-to-push-banks-to-remove-ibm-servers-in-spy-dispute.html. Zugriff: 26.08.2014.

[16] Shenzhen Daily (2010). „*Green Dam* office closed” http://paper.sznews.com/szdaily/20100714/ca294321.htm Zugriff: 04.09.2014.

[17] Jaume-Palasí, Lorena und Gierow, Hauke (2014). Germany; in Davies, Simon [Ed.]. “A Crisis of Accountability: A global analysis of the impact of the Snowden revelations”, 42- 46. http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf. Zugriff: 26.08.2014.

[18] Brito, Jerry und Watkins, Tate (2011). “Loving the Cyber Bomb - The Dangers of Threat Inflation in Cybersecurity Policy”, http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy Zugriff: 28.07.2014.

[19] Gorman, Siobhan (2009). “Security Cyber Czar Steps Down.” http://online.wsj.com/articles/SB124932480886002237. Zugriff am 28.09.2014 Zugriff: 28.09.2014; Higgins, Kelly Jackson (2012). „Obama Cybersecurity Czar Schmidt Steps Down.” http://www.darkreading.com/risk/obama-cybersecurity-czar-schmidt-steps-down/d/d-id/1137726 Zugriff: 28.09.2014.