merics
Mercator Institute for China Studies

China Monitor

Number 20 | 9 December 2014

Cyber Security in China: New Political Leadership Focuses on Boosting National Security

Restructuring internet regulation. Placing restrictions on foreign software. Developing the PRC's own IT standards.

by Hauke Johannes Gierow

MAIN FINDINGS AND CONCLUSIONS

- China's President and Party leader Xi Jinping has made cyber security a focal point in government work. Key high-ranking officials from numerous political sectors are involved in preparing and implementing cyber-security policy.

- Up until now, China has not pursued a coherent cyber security strategy. The lack of concentrated decision-making authority has resulted in inconsistent implementation of cyber security and in power struggles among various ministries.

- Xi Jinping has made the State Council Internet Information Office the key actor in the country's cyber security policy. Lu Wei, Head of the State Council Internet Information Office, is becoming increasingly prominent in internet policy.

- The Chinese government considers foreign software to be a potential threat to national security. Chinese businesses are encouraged to use domestic software, even though approved Chinese alternatives frequently do not perform as well and are not always as secure as Western products.

- The Chinese government's wish to regulate internet security as uniformly and comprehensively as possible conflicts with the security needs of individual internet users. Security gaps in mandatory (standard) software that users are forced to employ can become systemic points of penetration for hackers and malware.

- Beijing is steadily enlarging its radius of action in its cyber security policy. Developing internal security standards is certainly costly, but China is in fact becoming increasingly independent of the foreign IT industry.

1 "No National Security without Cyber Security."

"No national security without cyber security" (没有网络安全就没有国家安全), said President Xi Jinping to the state-run news agency Xinhua in April 2014.[1] The current leadership in Beijing clearly affords cyber security greater significance than only a few years ago. The Chinese government is increasingly resorting to protectionist measures to improve cyber security.

The Chinese government perceives software by Western manufacturers as a threat to national security. Therefore, its use in China is strictly regulated. The international implications of this regimentation are already becoming apparent. Chinese cyber security policy in general has the potential to alter the global market for IT products and services fundamentally.

China's government is currently taking concrete steps to enhance cyber security: in the spring of 2014, it founded the "Central Cyber Security and Informatization Leading Group" (中央网络安全和信息化领导小组). The fact that Xi Jinping has assumed leadership of this group illustrates the importance of the issue to the Chinese government. Xi is backed by Premier Li Keqiang, Liu Yunshan, First Secretary of the Central Secretariat of the Communist Party of China, and Zhou Xiaochuan, Governor of the People's Bank of China.[2]

2 Cyber Security – an Executive Responsibility

2.1 Basic Principles of Cyber Security Policy

The government in Beijing has been occupied with the issue of cyber security for more than ten years: as early as 2003, the "National Coordinating Small Group for Cyber and Information Security"（全国网络与信息安全协调小组） developed the first Chinese cyber security strategy. What is referred to as "Document 27" ("Opinions of the Leading Group for Strengthening Information Security Assurance Work", 国家信息化领导小组关于加强信息安全保障工作的意见) laid the foundation for several policy decisions which are still shaping policy today. Development of the cyber security policy has continued since Document 27 was enacted. The PRC's current cyber security strategy originates from 2012 ("Opinion of the State Council Concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security", 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]

This strategy defines a relatively broad range of objectives:

- boosting broadband expansion in China, particularly in rural areas;
- developing Chinese security technology;
- tightening control of the internet to "uphold good morals in the Net";
- researching next-generation mobile networks (5G);
- expanding e-government services in China.[4]

In addition, critical infrastructures are going to be protected and Chinese cryptographic standards developed in order to guarantee cyber security.[5]

2.2 Power Struggles over Cyber Security

Continually changing accountabilities and the dissolution of the first Leading Group in 2008 have resulted in a lack of concentration of decision-making competence in recent years. **Some ministries have attempted to fill this vacuum to secure their own position in the increasingly important field of Internet regulation.** Measures enacted by the political sector have not been implemented consistently as individual ministries put their own interests first. [6]

For example, to this day, different ministries have different security standards parallel to one another.

Companies trying to sell their technology to these ministries must undergo complex certification procedures and adapt their software wherever necessary in each particular case. Smaller IT start-ups in particular cannot afford this – many of them are therefore refraining from entering this quite lucrative public market sector. This is hampering the development of a strong Chinese IT sector.

Conflicts arise not only over responsibilities, but also over the issue of how far internet censorship should go. In the opinion of various decision-makers and local officials, strict control is hindering China's economic development. Voices within the government disagree on the "right balance". This conflict becomes apparent in the new free-trade zones, for instance. Press reports from Hong Kong indicate that internet censorship was originally to have been waived completely in the new financial free-trade zone in Shanghai. However, top officials denied this report later before state-run media. Local decision-makers from Shenzhen, in turn, announced that the free-trade zone Qianhai is going to waive internet censoring.[7]

2.3 Prioritizing Cyber Security under Xi

Several political actors are working on developing the state's cyber security policy. The "Central Cyber Security and Informatization Leading Group", which was called into being by President and Party leader Xi Jinping in 2014, brings high-ranking officials together with representatives of widely varying ministries (including representatives from the Ministries of Finance, Education and Culture as well as the National Development and Reform Commission).

The Leading Group is not an executive entity, but rather, it develops guidelines for the PRC's cyber security policy. Several members intentionally belong to several parallel groups such as the "Central Leading Group for Comprehensively Deepening Reforms" （中央全面深化改革领导小组, see MERICS China Monitor 13). This overlapping is intended to enhance transparency and encourage mutual cooperation.

The close connection of the Leading Group to the State Council Internet Information Office (now also called Cyberspace Administration of China,国家互联网信息办公室) is also expected to enable rapid implementation of guidelines and laws.[8]

Its chairman, Lu Wei, also heads the taskforce of the Leading Group and acts as coordinator of cyber security policy. Immediately following the 4th Plenary Session of the Central Committee of the Communist Party, he summoned representatives of local propaganda bureaus and councils for internet information as well as representatives of businesses and media from all of China for "discussions on the further juridification of cyberspace" (谈推进网络空间法治化).[9]

Fig. 1: Pioneers of China's Cyber-Security Policy. By Hauke Gierow

The example shows that Xi Jinping has advanced the State Council Internet

Information Office to the key actor of the PRC's cyber security policy.

The high-echelon membership of the new Leading Group and the coordinating role played by the State Council Internet Information Office send out strong signals within the political system: the Chinese government has recognized the importance of the topic and intends to eliminate existing deficits in the coming years. The prominent positions now held by many earlier pioneers of the PRC's cyber security policy also pave the way for new concepts (see Fig.1).

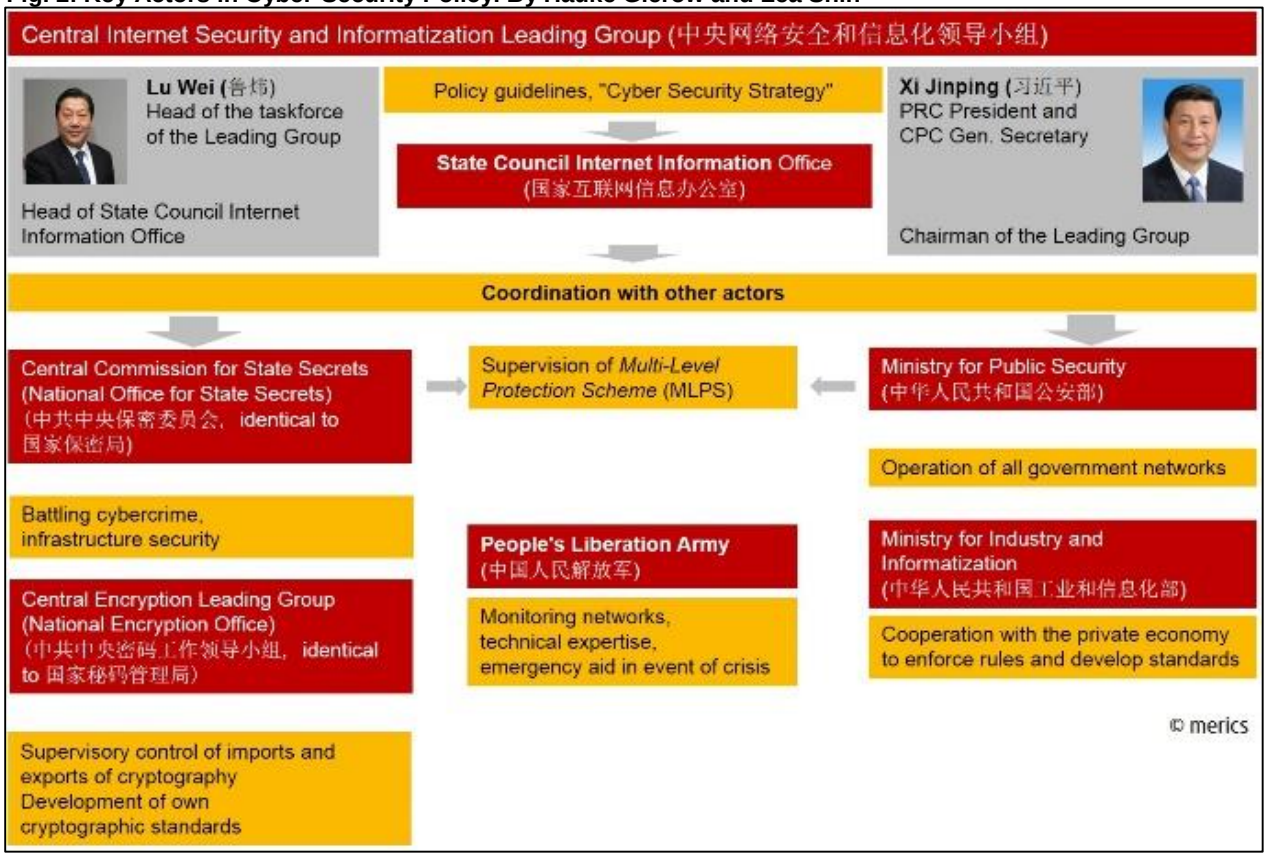
2.4 Security Sector Taking Responsibility

For the most part, in everyday work routines, the ministries responsible for cyber-security policy are those that already deal with security-related issues: the Ministry for Public Security (中华人民共和国公安部) is responsible for the areas of cybercrime, infrastructure security and – in collaboration with the Central Commission for State Secrets (中共中央保密委员会, identical with the National Bureau for State Secrets, 国家保密局) – the *Multi-Level Protection Scheme*, or *MLPS* (actually *Regulations on Classified Protection of Information Security*, 信息安全等级保护管理办法; a more detailed analysis is in Section 3).

The Ministry for Industry and Informatization (中华人民共和国工业和信息化部) coordinates cooperation with the private sector.

The General Staff Division of the People's Liberation Army (中国人民解放军总参谋部) mainly provides information about cyber attacks.

Fig. 2: Key Actors in Cyber-Security Policy. By Hauke Gierow and Lea Shih



It supports the Central Commission for State Secrets in the operation of classified government networks. Fig. 2 provides a detailed overview of the actors and their responsibilities.

3 Security Concerns or Industrial Policy?

3.1 The Multi-Level Protection Scheme (MLPS) *at the Heart of the Cyber Security Policy*

The key feature of current Chinese cyber security policy is to develop a high-powered domestic IT industry in order to stifle potential threats from foreign software. The MLPS is meant to help ward off this hazard.

Sectors crucial to security such as public authorities or strategically important companies must increase their deployment of technologies developed by Chinese citizens or companies. **This is expected to prevent foreign governments from gaining access to classified information through back doors.** The criteria for this originated from the certification process for "Document 27", which was published in 2003. Its application has been expanded continuously over the last few years.[10]

The Ministry for Public Security and the Office for Protection of State Secrets have been using the MLPS since 2008 to develop a process that provides IT security regulations categorized in different security levels. They apply to:

- private users and small companies (levels 1 and 2),
- businesses in strategically important sectors (finance, infrastructure and others; level 3)
- and public authorities (levels 4 and 5).

Figure 3 provides an overview of the criteria.[11]

The regulations have already had a **drastic impact on Western companies**: Microsoft can no longer sell its Windows operating system to Chinese officials, and manufacturers of anti-virus software such as Kaspersky and Symantec no longer have access to companies in security level 3.

Germany also has detailed regulations for secure IT products. Public IT contracts are only granted to companies that are in compliance with the so-called fundamental IT protection lists of the Federal Office for Information Security (BSI). The Common Criteria are similar regulations made at an international level.[12]

However, China purposefully distances itself from existing international agreements. Instead, Beijing has invested in the development of parallel IT standards such as WAPI for WLAN encryption and the alternative mobile telecommunications technology TD-SCMA.

Fig. 3: Criteria of the MLPS from level 3

No.	Criterion for security-related IT products
1	The product was developed by Chinese citizens, legal entities or companies with state participation.
2	China owns the intellectual property for key components of the technology.
3	Persons involved in the production process have no criminal record at all.
4	No back doors or Trojan horses have been built into the products.
5	The products pose no risk to national security, public order or public interests.
6	The software is certified for requirements of national security.

At the same time, the PRC applies the defined security criteria far more broadly than industrialized Western countries. Banks and other important companies in Germany and the United States also

have to meet IT standards, but the regulations there are less detailed and not categorized as strictly. Moreover, up to now, no country has ever been barred entirely from supplying IT products. Protectionist tendencies are recognizable not only in China, however, but also in the USA.

Seen from the Chinese government's perspective, restricting foreign software in sectors crucial to security is justifiable: operating systems and virus scanners in particular are potential weak spots and can permit virtually unlimited access to computers and server systems.

3.2 International Conflicts over IT Equipment

For years the United States has accused China of state-supported industrial espionage. The conflict escalated in the summer of 2014, when the American Justice Department prosecuted five alleged IT spies from China. In an indignant response, the leadership in Beijing alleged that the accusations were contrived.[13]

At this point, in light of the disclosures made by American whistle-blower Edward Snowden, the surveillance measures undertaken by the NSA also played into the hands of the Chinese government. Last year, they revealed that the US government had targeted weaknesses, including those in American hardware and software products, for espionage purposes. According to press reports, NSA employees even constructed these weaknesses intentionally, for instance in routers made by IT company CISCO.

Chinese IT companies have profited from the conflicts: the stock values of various companies such as Yonyou and Inspur rose considerably in 2014.

Fig. 4: An overview of the Multi-Level Protection Scheme. By Hauke Gierow. Source: footnote 10.

Level	Applies to	Impact of IT breakdown	Security requirements	Affected foreign software (example)
1 + 2	Private users / small and medium-sized companies	Isolated damage, no direct risk to society	Self-protection of users + companies, e.g. with firewalls / virus scanners	No regulations
3	Companies from the fields of energy, finance, transport, infrastructure	Hazardous to social order and public interest. Possible damage to national security	Regulations for access and use of systems, notification of public authorities concerning tests and security risks, annual security inspection	Foreign anti-virus software such as Symantec or Kaspersky, business software
4	Public authorities	Especially damaging for public interests / heavy damage to national security	Clearly defined levels of protection and access authorization, expanded security tests, "Trusted Computing" hardware. Security inspection every six months	Windows operating system + previous levels
5	Authorities with heightened security requirements	Particularly heavy damage to national security	Obligatory access control, minimal system complexity. Ongoing security inspection	Windows operating system + previous levels

One reason for this was that in response to the American activities, the Chinese government announced that the MLPS criteria would be applied more strictly and that promotion of the Chinese IT market would continue.[14]
The United States also limits imports of Chinese software for security reasons. As early as 2013, President Obama signed an act into law that prohibits acquisition of Chinese technology by American federal authorities. Private US companies are also encouraged to refrain from using Chinese technology.

3.3 Rules Are Detrimental to Competitiveness

Stricter application of the MLPS sometimes causes problems for Chinese companies. The reason for this is that technologies from the home country often do not offer users the same degree of sophistication that US products provide; sometimes even important functions are missing.
The Chinese government is willing to accept the disadvantages for companies and the high cost of adaptation. Conversion of IT systems can't take place overnight, even in China: at the China Postal Savings Bank, servers made by IBM are currently being replaced on a trial basis with products by the Chinese company Inspur. These tests are to be extended to other financial institutions in the medium term.[15]

4 Why Increased Surveillance and Control Do not Mean Increased Security: the Example of *Green Dam*

More state control of the internet does not necessarily mean more security for citizens. The introduction of software called *Green Dam* in 2009 illustrated this fact. Development of the software to enhance juvenile protection in the Net had begun in 2008 by order of the MIIT. It was supposed to block pornographic content automatically. On instructions from the MIIT, companies were required to equip all computers sold in the People's Republic of China with this program as of 1 July 2009. Computers in German schools also have comparable applications installed on them, but this is not mandatory.
In 2009, critics in China objected that the software further increases already stringent internet censorship as *Green Dam* also blocks websites that are critical of the government. Chinese IT-security experts also found serious security gaps which, due to the required pre-installation of the program, allowed hackers to take advantage of the security gaps to spy on all computers equipped in this way.
Not only *Netizens,* but also companies therefore protested loudly about the obligatory installation. In the end, the government withdrew the regulation only a few months after it had gone into effect. The companies that produced *Green Dam* have meanwhile gone bankrupt.[16]
This example goes to show that forced installation of uniform software can create an acute security problem. If all systems use the same software, then they are all vulnerable whenever errors occur. **The Chinese government's wish to regulate internet security as uniformly and comprehensively as possible conflicts with the security needs of individual internet users.**

5 Conclusion

The Chinese leadership is using its influence on all relevant institutions concerned with network regulation to implement extensive projects such as the MLPS. In the last few years, however, there has been a lack of political leadership necessary to enforce the measures decided upon.
The current government has recognized this deficit. Together with the new Leading Group and the strengthened role of the State Council

Internet Information Office , the government is taking concrete steps to improve internet security. Experts, however, are not sure if the sole use of nationally created software will indeed enhance cyber security.

Over the last few years, though, problems in implementing cyber security policy have not been restricted to China alone. Other countries are also experiencing difficulties, albeit in different areas. In Germany, for example, cyber security still is not a central political issue. Measures enacted by the federal government such as introducing a "no spying" provision or setting up a new, independent communications network for the federal government alone are considered by IT experts and public authorities such as the German Federal Audit Office to be half-hearted and ineffective. [17] In the United States, too, there has hardly been any movement at all in cyber security policy for years. Experts blame this on the close connection of private companies from the IT security sector with employees of the Administration, among other things.[18]The decision-making discretion available to the US government is limited by the importance of the IT sector – the United States cannot publicly question the security of its own technologies. Since no-one listened to them, several “Cyber Security Tzars” in the White House have already resigned. [19] Edward Snowden's disclosures have escalated the debate on the security of American software products – and could ultimately damage the competitiveness of America's IT industry.

China's build-up of its own IT industry will cause a major shift in existing global structures in the coming years. The highly focused industrial policy in support of the IT sector and the exports of Chinese technologies to partner countries in Africa and Asia have the potential of challenging and curtailing the dominance of the USA that has prevailed up to now in the IT industry.

Foreign companies must therefore expect a growing number of obstacles on the Chinese software market. If the present trend towards tightening Chinese security standards continues, the business environment will become even more problematical, particularly for US suppliers.

Several software producers from Europe such as SAP do not appear to have been affected by this situation very much up to now, probably because their products are still indispensable for many Chinese companies.

Contact for this issue of China Monitor:
Mr Hauke Gierow
hauke.gierow@merics.de

Publisher:
Mercator Institute for China Studies
Klosterstr. 64
D-10179 Berlin
phone: +49 30 3440 999-0
e-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 must evolve from a large internet nation to a powerful internet nation). http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm. Accessed on 28 September 2014.

[2] Xinhuanet (2014). "Xi Jinping leads Internet security group." http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm. Accessed on 16 June 2014.

[3]3 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." (Some Opinions Concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security). http://politics.gmw.cn/2012-07/17/content_4571519.htm. Accessed on 14 August 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." ("Opinion of the State Council concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security"). http://politics.gmw.cn/2012-07/17/content_4571519.htm. Accessed on 14 August 2014; Segal, Adam (2012). "China Moves Forward on Cybersecurity Policy." http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/. Accessed on 14 August 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." (Opinion of the Leading Group for Strengthening Information Security). http://www.360doc.com/content/14/0423/10/93013_371341672.shtml. Accessed on 14 August 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. Accessed on 14 August 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. Accessed on16 June 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/. Accessed on 5 September 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" (membership list of the Central Leading Group for Increasing Internet Security and Informatization: 12 top-ranking national-level politicians participate). http://www.guancha.cn/politics/2014_02_28_209672.shtml. Accessed on 5 September 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" (Director of the State Council Internet Information Office (Cyberspace Administration of China) in Beijing: Moving Forward the Discussion on the Juridification of Cyberspace). http://news.xinhuanet.com/politics/2014-10/26/c_1112981005.htm. Accessed on 28 October 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/. Accessed on 24 July 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" (Actions for Managing the Levels of Information Security). http://www.mps.gov.cn/n16/n1282/n3493/n3793/n494630/494907.html. Accessed on 5 September 2014

[12] For more on the Common Criteria, which were jointly agreed upon by Canada, France, Germany, the UK, the United States, Australia, New Zealand, Japan and Spain, see: Ernst, Dieter and 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. Accessed on 14 August 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. Accessed on 26 August 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/. Accessed on 24 July 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. Accessed on 26 August 2014.

[16] Shenzhen Daily (2010). "*Green Dam* office closed." http://paper.sznews.com/szdaily/20100714/ca294321.htm. Accessed on 4 September 2014.

[17] Jaume-Palasí, Lorena and 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. Accessed on 26 August 2014.

[18] Brito, Jerry and 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. Accessed on 28 July 2014.

[19] Gorman, Siobhan (2009). "Security Cyber Czar Steps Down." http://online.wsj.com/articles/SB124932480886002237. Access on September 28, 2014. Accessed on 28 September 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. Accessed on 28 September 2014.