MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

Perspectives on Cybersecurity:
A Collaborative Study

Massachusetts Institute of Technology:

Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz

Do Not Cite or Circulate Without Permission from Authors

Electronic copy available at: http://ssrn.com/abstract=2734336

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

PERSPECTIVES on CYBERSECURITY

A Collaborative Study

Authors

Chrisma Jackson

Lyla Fischer

Brooke Gier

Vivian Peron

Ben Ze Yuan

Liu Yangyue

Glenn Voelz

Editors

Nazli Choucri

Chrisma Jackson

Department of Political Science

MIT

2015

Electronic copy available at: http://ssrn.com/abstract=2734336

Table of Contents

Electronic copy available at: http://ssrn.com/abstract=2734336

6. China's Perspective on Cyber Security[87]

Liu Yangyue

China has become an increasingly important player in global cyberspace. By the end of 2014, China's online population has risen to 649 million, accounting for 19% of Internet users worldwide as seen in Figure 1. Chinese corporations in the IT industry have been active in making transnational acquisitions, providing services and content overseas, and enhancing technological competitiveness. In the international politics of Internet governance, China's influence is also on the rise in recent years, as it seeks for greater participation and agenda-setting capabilities through multilateral institutions. So is its impact on security issues of cyber politics. Given that great power politics has largely defined and shaped the scope and meaning of security studies, it is necessary to examine China's perspective and stance on cyber security before conceptual and practical frameworks on this issue can be developed.[88] So far, China has not published or clarified its national strategy on cyber security. However, several aspects make its perspective unique and may facilitate a more comprehensive understanding of cyber security.

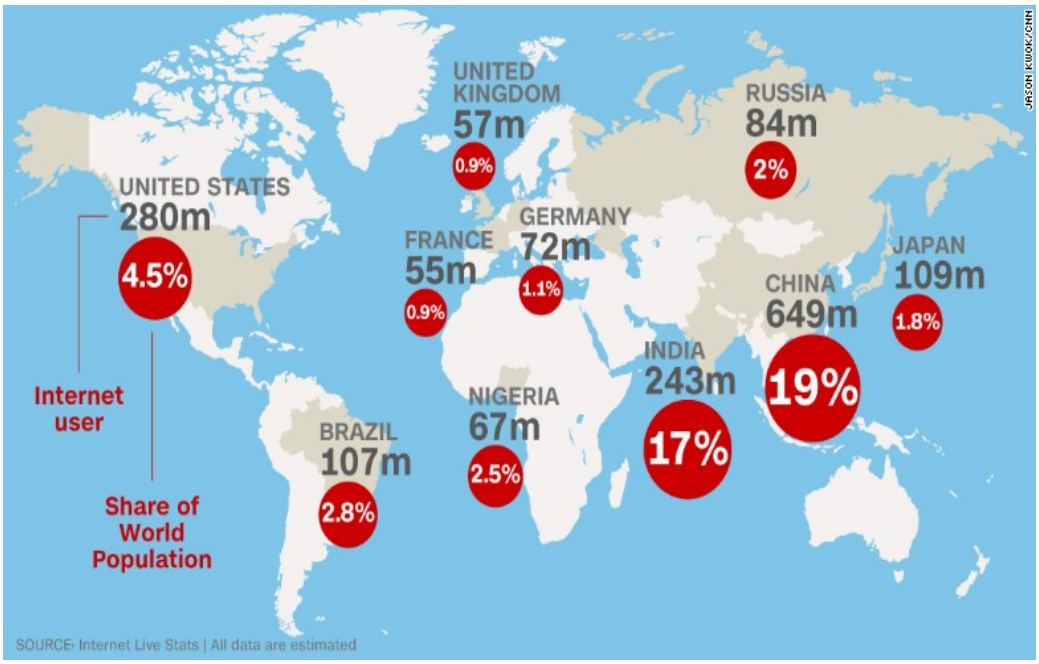


Figure 6.1
Global Internet usage
Source: Akamai (2014)

6.1 Internet Sovereignty

The first aspect concerns the notion of sovereignty. Unlike the Western mindset emphasizing the borderless nature of the Internet, what underlies the Chinese approach is the assumption that the

[87] Opinions and arguments expressed in this article are only personal, and do not represent any institution or government.
[88] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge, UK: Cambridge University Press, (2009), 50-53.

cyberspace is the natural extension, or a new dimension, of national sovereignty. In this sense nation-states should have unquestionable and paramount authority over the Internet system. In 2010, the Information Office of the State Council published a white paper on the *Internet in China*. Its content is to briefly outline China's stance on and understanding of Internet development and management. It contains a section called "Protecting Internet Security", in which it offers no clear definition of what Internet security is. However, it outlines three broad objectives of Internet security – respectively to "secure information flow", "combat computer crime" and "oppose all forms of computer hacking".[89]

These objectives make China's understanding of Internet security almost identical with other countries. But a notable difference lies in the emphasis on the Internet sovereignty. In the white paper, it proclaims "the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected". Meanwhile, "citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security".[90]

By asserting sovereignty over cyberspace, China has re-framed the Western norm of a market-based, borderless Internet system to a reverse side that weighs national security over liberty and freedom. Moreover, the notion of Internet sovereignty would indicate a more centralized management system rather than distributed and decentralized governance. In fact, the design and structure of cyberspace do not necessarily favor a particular governance mode over others. As Rebecca MacKinnon has commented on Internet sovereignty, "it's a physical reality that web sites have to be hosted physically on computers that are located in some jurisdiction or another; they are operated by physical human beings who reside under a government jurisdiction and can thus be physically controlled when necessary; they are operated by businesses that have to be registered in one or more jurisdiction and their physical operations are subject to government regulation; and the Internet runs on networks that physically exist within or pass through nation-states".[91]

These connections between physical existence and virtual space mean that sovereignty can still be practiced, to some extent, in the cyber domain. A typical example refers to the way in which critical resources related to the operation of the Internet system are distributed and managed. On this score, the white paper outlines a hierarchical model of resource allocation by announcing, "the state telecommunications administration department is responsible for the administration of the Internet industry, including the administration of basic resources of the Internet such as domain names, IP addresses within China".[92] In China, the allocation and administration of domain names and IP addresses are controlled by the China Internet Network Information Center (CNNIC), which serves as a bureaucratic subordinate of the Ministry of Industry and Information Technology (MIIT). It should be noted that the global allocation of IP addresses is implemented in a geographic manner. It is divided into several Regional Internet Registries, with CNNIC being vertically affiliated to Asia-

[89] Information Office of the State Council of China. *The Internet in China*.. (2010): White paper available at http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.
[90] Ibid.
[91] Rebecca McKinnon, "China's Internet White Paper: networked authoritarianism in action," *RConversation* (blog), June 15, 2010, http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.
[92] Information Office, *The Internet in China*.

Pacific Network Information Center (APNIC) in Australia.

Ownership represents another mode of Internet sovereignty. In this regard, the Regulation on Telecommunications in China differentiates between two types of telecommunication services, basic telecom service (provision of public Internet infrastructure) and value-added service, and stipulates that companies in the basic telecom service should have at least 51% of their shares owned by the state. By putting service providers under national jurisdiction and control, this approach ensures that territoriality still matters when dealing with the virtual domain.

The notion of sovereignty has significant implications for the understanding of cyber security. It delineates a different boundary for where insecurity resides. It makes the distinction between globalized space and imagined national boundary. Sovereignty lies at the national side, which implicitly or explicitly portrays nation-states as the core referent object. Crucial factors that sustain the national image of cyber security point to the physical infrastructure of cyberspace which still operates within national borders, as well as the fundamental roles of territorial government that persist in the cyber domain.[93] On the other hand, cyber security also represents a novel global issue that occurs in a new arena of interactions.[94] Norms, practices, and institutions that manage security problems in the cyber domain have been fundamentally transformed due to the globalized feature of the cyber system.[95] The global governance of cyberspace may indicate the de facto elimination of cyber security boundary. This division, however, has also inhibited global efforts to establish a cohesive and coordinated framework that can better address cyber security problems. Recent development in global Internet governance regime, including events such as the WCIT in 2012 and NetMundial in 2014, has seen increasing disputes and disagreements about the future of Internet management.[96] How to bridge and conciliate these different visions would prove crucial in facilitating international cooperation on cyber security.

6.2 Information Security

Information security is another important element in China's perception of cyber security. Information security portrays information, per se, rather than its transmission as the major security concern. More specifically, it focuses primarily on the content and values embedded in the digital information.

The Administration of Internet Information and Service Procedures, promulgated in 2000, have broadly defined nine types of unlawful online content, including any content that opposes the fundamental principles of the Chinese Constitution, compromises state security, undermines national unity, and harms the dignity and interests of the state.[97] In an updated revision five year later, two additional materials are banned in cyberspace, namely any information that would incite illegal assemblies, marches and demonstrations, and that would represent the agendas of any illegal civil groups. In 2004, the China Internet Illegal Information Reporting Centre (CIIRC) was established to

[93] Daniel Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119, No. 3 (2004): 477-498; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press).
[94] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012).
[95] John Mathiason, *Internet Governance: The New Frontier of Global Institutions* (London: Routledge, 2008); Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010).
[96] Alexander Klimburg, "The Internet Yalta," *Center for a New American Security Commentary* (2013).
[97] Information Office, *The Internet in China*.

police the Internet space and identify any unlawful online materials.

To strengthen information security and enforce content regulation, China has built a multi-layered system. At the top level is a pervasive and effective filtering mechanism. Since 1998, the Ministry of Public Security has developed a powerful filtering and blocking system to monitor information flows between China and the outside world. This project, known as the Golden Shield, has become one of the most sophisticated and effective checkpoints in the information network. According to a report by the Open Net Initiative, although China is not the only country that deploys filtering techniques, "it is unique in the world for its system of Internet connections when triggered by a list of banned keywords".[98] This system is implemented at the backbone level, using a method named TCP resets. It can inspect the content of transmitted packets to uncover whether sensitive keywords are present and thus disrupt the connection. Using this filtering system, the government could contain undesired online discussion and communication, especially during politically sensitive periods or in times of emergency. This mechanism has also enabled the government to wipe out controversial news and anti-government speeches on the Internet ahead of important political events.

Below that level, responsibilities for regulating online information are delegated to content and service providers. For instance, major content providers are required to build internally a monitoring department. People in such department are in charge of examining and authorizing the information to be posted on their platform / website. Recent research by Gary King and his colleagues focus on the provider-level of information regulation.[99] It shows that the objective of regulation is mostly to reduce the likelihood of offline collective action mobilized through online platform. By contrast, criticism of the state or the Party has no evident effects on triggering regulatory measures. This finding indicates that the major concern of information security for China is to maintain social and political stability. On this score, political development in Egypt, Libya, Syria, Thailand and other countries may have served as a warning. Although information technologies may have empowered civil society vis-à-vis, the state, political order could be much more difficult to rebuild than collapse.

Teams of online commentators are also established by websites, media, government agencies as well as other state-sponsored institutions. Their duty is to guide and shape online opinion by countering rumors and developing positive arguments. The ultimate goal is to build a harmonious Internet space that supports rather than undermines existing socio-political structure. In late 2007, Cai Mingzhao, then-Vice Director of Information Office of State Council, emphasized that all forms of Chinese online media should "have a firm grasp of correct guidance, creating a favorable online opinion environment for the building of a harmonious society".[100] Down to the user-level, regulatory measures also include mechanisms such as real-name registration and filtering software.

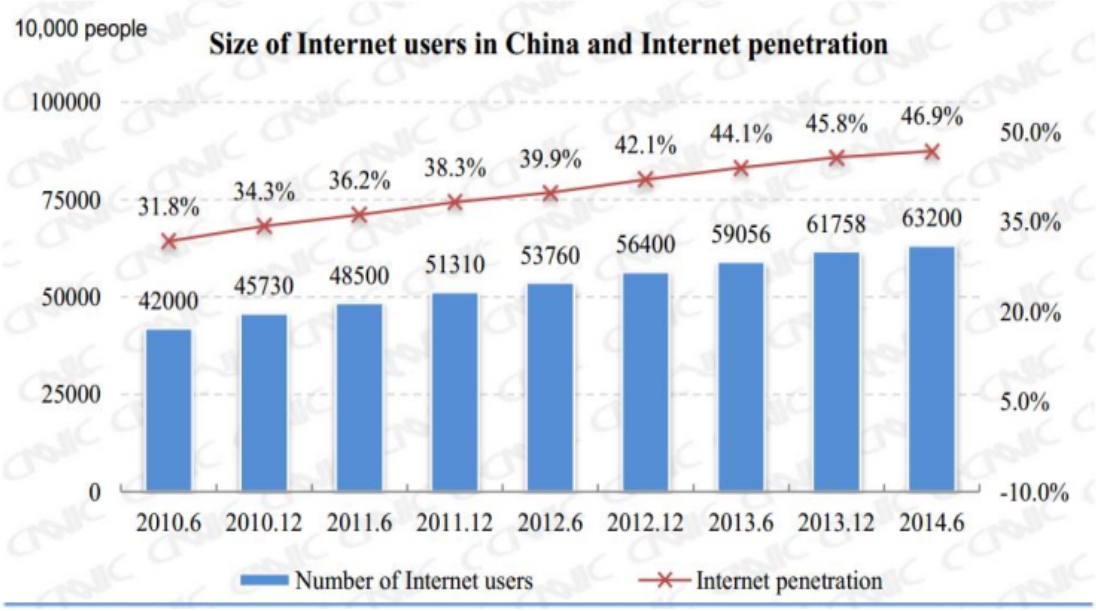
The emphasis on information security makes China's perspective on cyber security different from that of the Western countries. While cyber security in the West is largely understood as concerning the rights of the individual, in the Chinese context it highlights collective, societal

[98] "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," Open Net Intitiative, accessed on…… https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.
[99] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (2013): 1-18.
[100] David Bandurski, "State Council Vice-Minister reiterates control as top priority of Internet development in China," *China Media Project* (December 2007): http://cmp.hku.hk/2007/12/04/763/.

security, which places stability as a higher priority. Therefore, the 2010 white paper stresses "the free and safe flow of Internet information is integrated as a whole. On the premise of protecting the safe flow of Internet information, the free flow of Internet information may be realized".[101] This aspect of cyber security conception is not unique to China. Countries such as Russia also regard cyberspace as an integrated part of information space, where human cognitive processes interact with all kinds of information. In this sense, cyber security should not be separated from information security that deals with information systems as well as human minds.[102]

6.3 Development and Security

Last but not least, there is also a development aspect of cyber security. Over the past decade, the Internet in China has experienced high-speed growth (Figure-2). China now has the world's largest population – both online and offline. However, there is still a significant gap between China and more industrialized countries in terms of infrastructural development. Table 1 below exhibits several indicators related to Internet development among selected countries. It shows that China is still lagging behind in terms of secure servers, Internet hosts, and connection speed. For instance, China possesses only four secure Internet servers per million people, while that number is 1,306 for the United States, and 1,995 for South Korea. It is also noticeable that the use of pirated software prevails among Chinese Internet users (although not shown in the table). This has at least two implications for security: first is that the cyber environment in China is vulnerable. Akamai's quarterly reports of Internet attack traffic often identify China as one of the major attack sources (Table 1). But the nature of botnet suggests that the traced attack sources can also be (unwittingly) victims of intrusions and hijacks.



[101] Information Office, *The Internet in China*.
[102] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *5th International Conference on Cyber Conflict*, eds. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE publications, 2013).

Source: CNNIC (2014)

Figure 6.2
China's Internet Growth

Table 1 Selected Indicators of Internet Development

	China	U.S.	Russia	Japan	S. Korea
Secure Internet servers (per 1m people)	4	1,306	51	737	1,995
Internet hosts (m.)	20.6	505	14.9	64.5	0.3
Average connection speed (Mbps) (2014Q4)	3.4	11.1	9	15.2	22.2
% of attack traffic (2014Q4)	41	13	3.2	0.8	2.8

Source: World Bank (2013); CIA World Factbook (2012); Akamai (2014)

Secondly, it creates a sense of technological dependency. For example, China has realized for a long time that in the areas of critical information technologies, such as CPU (central processing unit) and operating systems, it is highly dependent upon foreign companies. The risk of such dependency for national security has been recognized long ago. According to a survey conducted by a Chinese government agency, 97% of operating systems, 87% of servers, and a majority of industrial control systems currently used in China are overseas products. In a 2014 speech at the Leading Group for Informationization and Network Security, President Xi Jinping stresses that "cyber security is critical for national security and development … To build a cyber great power, China has to develop its own technologies".

In fact, China has made great efforts to promote security through indigenous innovations. One example is the WAPI standard. WAPI, short for WLAN Authentication and Privacy Infrastructure, is a Chinese-developed standard used for wireless networking system. It was allegedly designed to overcome the security deficiencies of the widely used Wi-Fi standard which was approved by the Institute of Electrical and Electronics Engineers (IEEE) in 1999. China initially announced in 2003 that all wireless devices sold in the Chinese market should support the WAPI standard. This move threatened the interests of the "Wi-Fi coalition" and provoked strong protest from the United States.[103] In 2004, the U.S. Secretary of Commerce Donald L. Evans, the Secretary of State Colin L. Powell, and the Trade Representative Robert B. Zoellick jointly sent a letter to their Chinese counterparts, complaining about the mandatory WAPI policy as a technological barrier to international trade.[104]

Under tremendous diplomatic pressures, China postponed the implementation of such a policy,

[103] Scott Kennedy, "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars", *Asia Policy* 2 (July 2006): 41-62.
[104] Sumner Lemon, "U.S. Government Voices Opposition to China's WLAN Standard", *IDG New Service* (March 2004): http://www.infoworld.com/t/networking/us-govt-voices-opposition-chinas-wlan-standard-740.

but later changed its tactic from internationalizing the WAPI standard to popularizing it first in the domestic market. Meanwhile China launched several prominent projects to make the WAPI a de facto mandated and industrialized standard, especially the extensive application of the WAPI in the 2008 Beijing Olympic Games and in the government procurement. This political effort paid off in 2009 when ten major countries, including the United States, and major industrial giants like Intel and Broadcom, had agreed to promote the WAPI as an international standard.[105] However, the Chinese government's effort to internationalize the WAPI standard suffered a temporary setback in mid-2011 when the United States rejected the visa of a Chinese expert who planned to raise the WAPI issue at the International Standard Organization's conference in San Diego.

The WAPI case is only one story of China's efforts to enhance indigenous innovations. Other achievements (as well as setbacks) have also occurred in the development of CPU, operating systems, technical standards, and high performance computers. The concern of technological independence has played an important role in China's policy of cyber security. Especially after the Snowden affair, Chinese government procurement has banned a number of overseas products, like the Windows 8 operating system, McAfee and other anti-virus software, CISCO's routers etc. And China is building an information technology review system to decide whether certain IT products are secure before they can be imported. All these developments are in the same line as China's pursuit of technological independence, which has been considered as a critical part of cyber security. In this sense, the recent U.S. embargo of processors widely used in the Chinese supercomputing industry may only validate and deepen China's concern about technological dependency.

6.4 Concluding Remarks

Although authoritative account in China has not provided a single, clarified (and publicly available) definition of cyber security, three aspects make its perspective distinctive. The elements of Internet sovereignty, information security and development are not separated from each other. Information security illustrates China's primary concern of Internet-related security problems, which prioritizes order and stability. Sovereignty represents an imagined domain, bounded by implicit and explicit nodes and scope, that falls under state jurisdiction and protection. Development, especially in terms of technological independence, is embedded in the conception of security and regarded as the most reliable and sustainable means to security.

Discussions above may have some interesting implications for the understanding of cyber security. While cyberspace is often perceived as a public domain where ownership and hierarchical authority do not apply, it is also an interactive system that has profound effects upon socio-political systems. Should inherent features of a socio-political system, such as culture, political order, and social stability, be part of the cyber security referent object? Should development and distribution be integrated into the conceptualization of cyber security? If so, what impacts would it bring to the current global regime of Internet governance? These questions are only a small fraction of puzzles emerging from the development of information technologies. It is of great necessity to enhance multilateral and multi-level dialogue and theory-building efforts to better understand the new issues in

[105] Iris Hong, "China's WAPi standard wins international support", *Telecomasia.net* (June 2009): http://www.telecomasia.net/content/chinas-wapi-standard-wins-international-support.

cyber politics.

As an added set of observations, the following is presented:

- Cyber Security and Global Governance
    - The white paper (2010) : “China maintains that all countries should, on the basis of **equality and mutual benefit**, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security… China holds that **the role of the UN** should be given full scope in international Internet administration… China maintains that all countries have equal rights in participating in the administration of the fundamental international resources of the Internet, and a **multilateral and transparent allocation system** should be established on the basis of the current management mode, so as to allocate those resources in a rational way and to promote the balanced development of the global Internet industry.”
- Cyber Security and Global Governance
    - China, Russia and other SCO members submitted the *International code of conduct for information security* in 2011 and 2015;
    - Code of Conduct: “Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security”; and not to “interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability”.
    - “All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development”.
- Cyber Security in Different Contexts
    - Cyber security for whom? Should culture, political order, social stability etc. be part of the cyber security referent object?
    - As the “freedom from fear” and “freedom from want” are intrinsically intertwined, the issue of development also plays a role in dealing with cyber security.
    - To what extent does power politics matter in global Internet governance?
- Sovereignty and Cyberspace
    - Krasner (1999) named four types of sovereignty: **domestic sovereignty** – actual control over a state; **interdependence sovereignty** – actual control of movement across state's borders; **international legal sovereignty** – formal recognition by other sovereign states; **Westphalian sovereignty** – lack of other authority over state than the domestic authority.
    - Is sovereignty feasible in cyberspace? Is cyberspace exerting a qualitative or quantitative impact on sovereignty

References

Bandurski, David. 2007. State Council Vice–Minister reiterates control as top priority of Internet development in China. *China Media Project*. (December): http://cmp.hku.hk/2007/12/04/763/.

Buzan, Barry and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge, UK: Cambridge University Press.

China Internet Network Information Center. 2000. *State Council Article 15, Administration of Internet Information and Service Procedures.* (September): http://www.cnnic.net.cn/html/Dir/2000/09/25/0652.htm.

China Internet Network Information Center. 2014. *Statistical Report on Internet Development in China*. http://www1.cnnic.cn/IDR/ReportDownloads/201411/P020141102574314897888.pdf.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Drezner, Daniel. 2004. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly* 119 (3): 477-498.

Giles, Keir and William Hagestad II. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, and M. Maybaum eds., 5th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf

Goldsmith, Jack L. and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press.

Hong, Iris. 2009. China's WAPI standard wins international support. Telecomasia.net (June): http://www.telecomasia.net/content/chinas-wapi-standard-wins-international-support.

Information Office of the State Council of China. 2010. *The Internet in China*. White paper available at: http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.

Kennedy, Scott. 2006. The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars. *Asia Policy* 2 (July): 41-62.

King, Gary, Jennifer Pan, and Margaret Roberts. 2013. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, 107 (May): 1-18.

Klimburg, Alexander. 2013. The Internet Yalta. *Center for a New American Security Commentary*. (February): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf

Lemon, Sumner. 2004. U.S. Government Voices Opposition to China's WLAN Standard. *IDG News Service* (March): http://www.infoworld.com/t/networking/us-govt-voices-opposition-chinas-wlan-standard-740.

MacKinnon, Rebecca. 2010. China's Internet White Paper: networked authoritarianism in action. Web blog *RConversation*, June 15. http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. London: Routledge.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Open Net Initiative. "China's Green Dam: The Implications of Government Control Encroaching on the Home PC." Accessed on ……., https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Xinhuanet. 2014. Xi Jinping leads Internet security group. (February): http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.