Cybersecurity in the Chinese Context

Changing Concepts, Vital Interests, and Prospects for Cooperation

Cai Cuihong

Abstract: “Cybersecurity” has become a topic of great strategic importance concerning both national and international security, especially after Edward Snowden’s disclosure of the secret surveillance programs of the U.S. government. With the largest number of netizens in the world, China holds its own views, beliefs, and assumptions on this topic. To understand the current disputes over international cybersecurity and to identify challenges and opportunities presented to international cybersecurity cooperation, it is of great significance to examine “cybersecurity” in the Chinese context. This article deals with the following issues from a Chinese perspective: cyberspace and cybersecurity in general, China’s vital

Cai Cuihong is Associate Professor at the Center for American Studies, Fudan University. chcai@fudan.edu.cn; Center for American Studies, Fudan University, No. 220, Handan Road, Shanghai 200433, China

This paper was first presented at the Berlin Conference on Asian Security (BCAS, June 14-16, 2015) jointly organized by the *Stiftung Wissenschaft und Politik* (SWP) and the *Konrad-Adenauer-Stiftung* (KAS). The author would like to thank the anonymous reviewers of the journal, the commentators at the 9th BCAS as well as Professor Mel Gurtov at Portland State University for their valuable comments.

This research is supported by a grant from the China National Social Sciences Fund “Cyberpolitics in US-China Relations in the 21st Century” (Award no. 12BGJ018).

cybersecurity interests and threatening challenges, and barriers to further progress in international cybersecurity cooperation. It is concluded that China's understanding of cybersecurity, which derives from its unique national conditions, does not limit its willingness to participate in international cybersecurity cooperation.

Keywords: Cybersecurity; cyberspace; "Holistic National Security Outlook"; information security.

Introduction

A series of measures with regard to cybersecurity recently taken by the Chinese government indicate the growing significance of the issue. The establishment of the Central Leading Group for Cyberspace Affairs¹ in February 2014 might be the most notable one. President Xi Jinping, acting personally as the group leader, proposed a critical thesis of "No cybersecurity, no national security; no informatization, no modernization."² President Xi's remarks at the group's first meeting demonstrated the maintenance of cybersecurity as a priority on China's political agenda, signaling a new, high-level prioritization of cyber as a major strategic initiative with political, economic, and military implications. As Mr. Lu Wei³ pointed out,

Network security has gone beyond the scope of technology, with more decisive significance. It entails innovation, protects development and leads technology. It is the forerunner of the market as well as the symbol of core competitiveness.⁴

¹This is the official translation of "zhonggong zhongyang wangluo anquan yu xinxi hua lingdao xiaozu," literally meaning the "central leading group on network security and informatization."

²See President Xi Jinping's speech at the first session of the Central Leading Group for Cyberspace Affairs, Cyberspace Administration of China website, February 27, 2014, http://www.cac.gov.cn/2014-02/27/c_133148354.htm.

³Lu Wei is Director of the Office of the Central Leading Group for Cyberspace Affairs, Director of the Cyberspace Administration of China, and Vice Minister of CPC's Publicity Department.

⁴See Lu Wei's keynote speech at the China-ROK Internet Roundtable Conference, *Xinhua News*, December 10, 2013, http://news.xinhuanet.com/world/2013-12/10/c_118489322.htm.

In addition to the official statements concerning cybersecurity, many other policies adopted in the past two years also highlight the importance the Chinese government has attached to Internet security.⁵ Since China's actions on cybersecurity have been attracting world attention, it is necessary to examine the Chinese thinking behind them. What are the Chinese perspectives on cybersecurity? What are the major challenges that China perceives to cybersecurity? And what are Chinese positions on international cybersecurity cooperation? Mainly based on Chinese-language literature, this paper tries to explore the answers to the above questions in order to facilitate the understanding of current disputes on international cybersecurity, and find out the challenges and opportunities presented to international cybersecurity cooperation.

Chinese View on Cyberspace & Cybersecurity

Distinctive national conditions of China lead to its different perspectives or perceptions from those of Western countries on cybersecurity. In the Chinese context, rather than a technological issue, cybersecurity is a strategically important subject concerning social governance.

From Information Security to Cybersecurity

Internet security, network security, as well as cyberspace security are interchangeable terms for "*wanglu anquan*" (cybersecurity) in the Chinese lexicon. It is not easy to find appropriate Chinese terms that fully convey the meaning of "cybersecurity," and there is no official definition with respect to the concept of "cybersecurity," although the draft Cybersecurity Law tries to make such efforts. The choice of words has been in constant development and has undergone many changes. In the early years of stand-alone computers, the common expressions for security issues were "communication security" and "computer security." "Regulations of the People's Republic of China on the Protection of Computer Information System

⁵For example, China's First National Cybersecurity Week was observed in November 2014, and the second one was observed in June 2015, both aimed to promote nation-wide cybersecurity consciousness.

Security,” issued by the State Council in 1994, employed the phrase combining “computer security” and “information security.”

In China’s official context, the Cyberspace Administration of China has the responsibility to manage Internet content and safeguard information security, while Internet technology management constitutes part of the mandate of the Ministry of Industry and Information Technology. Nevertheless, the media and the academia usually regard “information security” as the mainstream term, especially before 2014.⁶ To echo the Western lexicon and better interpret diversified aspects of the issue, the Chinese government has adopted the term of “cybersecurity,” although in some official documents released in 2014 “information security” was still widely used. For example, in the document of

“Information security” in the Chinese context highlights the state’s control of information flow, while “cybersecurity” signifies the robustness of network systems.

“Instructions on Further Strengthening Military Information Security,” issued by the Central Military Commission in October 2014, the term “information security” was included. It also appeared in the statement of the first session of the Central National Security Commission held in April 2014.

As for the legal interpretation in Chinese, “network” tends to emphasize network hardware and network space, while “information” mainly focuses on data information on computer networks, which is usually referred to as “content.” Each of these terms stresses different aspects. Traditionally, the Chinese government prefers to use the concept of information security, with a view to protecting ideological security and emphasizing state control and dominance over information flow. When addressing the audience at the China-ROK Internet Roundtable Conference on December 10, 2013, Lu Wei commented that “Information is the ‘blood’ of the Internet. The Internet will be lifeless without the security of information content.”⁷

⁶Cui Guangyao, “Xinxi Anquan Yinxiang 2014 [An Annual Review of Information Security in 2014],” *China Information Security*, No. 1 (January/February 2015), p. 51.

⁷See Lu Wei’s speech at the China-ROK Internet Roundtable Conference, *Xinhua News*, December 10, 2013, http://news.xinhuanet.com/zg/jx/2013-12/12/c_132961157.htm.

The concept of cybersecurity has also been evolving in recent years. The previous term for cybersecurity, better interpreted as network security, was a purely technical term, but now comprises meanings not only related to technology, but also human behavior, as well as the relationships between different actors. In the technical sense, cybersecurity means that the network system's hardware, software, and its system data are protected against any destruction, alteration or disclosure for accidental or malicious reasons; meanwhile the systems remain continuous and reliable, and network services are without any interruption. From the perspective of orderliness, cybersecurity shows an orderly fashion in which users are able to carry out a variety of activities in cyberspace. These two types of security are inextricably linked and mutually reinforcing. The steadiness of orderly security is based on technical security, while the progress of technical security depends on the guarantee of orderliness. Only by taking both types of securities into account will the network be able to achieve maximum security.

Network Sovereignty and Cybersecurity under the “Holistic National Security Outlook”

Since 2014, the “Holistic National Security Outlook” (*Zongti Guojia Anquan Guan*) have started to serve as the guiding principle of China's national security. When chairing the first session of the newly established National Security Commission on April 15, 2014, President Xi put forward the “Holistic National Security Outlook,” pointing out the needs to build a national security system comprised of political security, homeland security, military security, economic security, cultural security, societal security, science and technology security, information security, ecological security, resource security as well as nuclear security. Summarized in 71 Chinese characters by President Xi, the “Holistic National Security Outlook” is translated into brief English as

Place equal emphasis on external security and internal security;
place equal emphasis on homeland security and national security;
place equal emphasis on traditional security and non-traditional security; place equal emphasis on development issues and

security issues; place equal emphasis on self-security and common security.⁸

Cybersecurity is apparently linked to almost every aspect of China's national security system. Furthermore, cyberspace is the domain where new situations, problems, features and trends are manifested in most cases. President Xi's statement of "no cybersecurity, no national security" indicates the inherent links between cybersecurity and national security in various domains. Based on the "Holistic National Security Outlook," combined with China's national conditions, China hopes to clarify the relations between cyberspace and national sovereignty.

The Chinese government believes that the Internet is an important infrastructural 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.⁹

Meanwhile, China is opposed to absolute network security, believing that "there should not be double standards in the field of information, and no nation shall seek its own allegedly absolute security at the expense of other countries' security."¹⁰

Thus, in the congratulatory letter sent to the first World Internet Conference held on November 19, 2014, President Xi also

China places
network sovereignty
before cybersecurity
concerns.

⁸See President Xi Jinping's speech at the first session of the National Security Commission, "Jianchi Zongti Guojia Anquan Guan, Zou Zhongguo Tese Guojia Anquan Daolu [Adhering to the Holistic National Security Outlook on the Path of National Security with Chinese Characteristics]," *People's Daily Online*, April 15, 2014, <http://politics.people.com.cn/n/2014/0416/c1024-24900227.html>.

⁹Information Office of the State Council of the PRC, *The Internet in China*, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm.

¹⁰In his speech at the Brazilian National Congress, Xi Jinping made the case for building on the traditional friendship between Brazil and China to jointly write a new chapter in the bilateral relationship, see "Xi Jinping Tan Hulianwang Zhili [Xi Jinping Speaks on Internet Governance]," *Sina News*, July 18, 2014, <http://news.sina.com.cn/c/2014-07-18/184230543560.shtml>.

placed the significance of respecting network sovereignty before that of maintaining network security.¹¹ He stated that “China is willing to deepen cooperation with other countries, to respect network sovereignty, and to maintain network security.” In the China-ROK Internet Roundtable Conference held on December 10, 2013, Lu Wei raised four proposals, the first among which is “to jointly safeguard the security of network sovereignty.” He noted that the rapid development of Internet technology has naturally extended the scope of national sovereignty to cyberspace. Information service is able to transcend national borders, while cyberspace cannot exist without sovereignty.¹² Lu Wei also noted in his keynote speech in the First China-ASEAN cyberspace forum held on September 18, 2014, that

Information dissemination has no national borders, but cyberspace does have boundaries, and therefore we have to respect the network sovereignty of each country.¹³

Informatization and Cybersecurity of a “Cyberpower”

Since the inauguration of the Central Leading Group for Cyberspace Affairs in February 2014, President Xi has vowed to pursue the strategic goal of transforming China into a cyberpower.

This goal includes two specific aims. One is to become a great power in cyberspace, and the other is to acquire national power by making full use of the Internet. In general, the status symbols of a cyberpower include, at least, a globally competitive Internet industry, full defensive capabilities for key national

¹¹See President Xi Jinping’s message of congratulations to the First World Internet Conference, *Xinhua News*, November 19, 2014, http://news.xinhuanet.com/live/2014-11/19/c_127228771.htm.

¹²See Lu Wei’s speech at the China-ROK Internet Roundtable Conference, December 10, 2013 *Xinhua News*, http://news.xinhuanet.com/world/2013-12/10/c_118489322.htm.

¹³See Lu Wei’s keynote speech at the First China-ASEAN Cyberspace Forum, Information Office of the State Council of the PRC website, September 18, 2014, <http://www.scio.gov.cn/zhzc/8/5/Document/1381275/1381275.htm>.

infrastructure, and adequate deterrence in terms of cybersecurity and military security.¹⁴

The “cyberpower” status does not imply that China will impose its own cyberspace doctrines upon other countries. It only means that China will acquire sufficient cyber capabilities to be self-sufficient. This strategic goal is set out based on an assessment of the status quo in which China possesses a wealth of cyber infrastructure but still relies on foreign products.

This strategic goal also envisions “informatization” and “cybersecurity” as two sides of the same coin. China attaches equal importance to either of them. Cybersecurity and informatization are sometimes analogized as “two wings on one plane, two wheels on one motorcycle,” which must be taken under unified planning, unified deployment, unified propulsion, and uniform implementation. In the first session of the Central Leading Group for Cyberspace Affairs, President Xi emphasized:

No cybersecurity, no national security. No informatization, no modernization. Only by using security to guarantee development and using development to promote security, can long-term peace and order be realized.¹⁵

The Communist Party of China fully understands that its political legitimacy does not hinge on ideology, but on the long-term economic development and social progress. In this sense, China is not willing to regulate cyberspace at the expense of economic and social development. Therefore, China’s cyber policy

China’s cyber strategy reflects its ambition both to become a major power in cyberspace and to enhance its national power through cyber development and application.

¹⁴Fang Xingdong and Hu Huailiang, *Wangluo Qiangguo: Zhongmei Wangluo Kongjian Da Boyi* [Cyberpower: The Grand Bargain between China and the United States in Cyberspace], Beijing: Publishing House of Electronic Industry, 2014. Preface, p. ix.

¹⁵See President Xi Jinping’s speech in the first session of the Central Leading Group for Cyberspace Affairs, Cyberspace Administration of China website, February 27, 2014, http://www.cac.gov.cn/2014-02/27/c_133148354.htm.

could be interpreted as fundamentally pragmatic. Network development and informatization are conducive to social and economic development, and are thus helpful for strengthening political legitimacy. Aiming at further promoting economic and social development via leverage of the Internet, China's "Internet Plus" initiative has sparked off nation-wide discussions. Based on the Internet platform, this initiative

employs the cross-border integration of information and communication technology with a variety of industries, thereby promoting industrial restructuring and upgrading, continuing to create new products, new business and new models, and building a nascent ecosystem that connects them all.¹⁶

In addition, the application of information technology for military purposes is also an essential safeguard for cybersecurity. In *China's Military Strategy*, a white paper published in May 2015, cyberspace is defined as a new pillar of economic and social development, as well as a new domain of national security.

As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situational awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.¹⁷

China still has a long way to go in terms of informatization. As indicated by the "Measuring the Information Society Report 2014" issued by the International Telecommunication Union, China ranks 86th in the Information Development Index. "The Global Information Technology Report 2014" ranks China 62nd in the Networked Readiness Index. "The Global E-Government Survey 2014" issued by the United Nations

¹⁶Si Xiao *et al.*, "Hulianwang + Shi Shenme [What is "Internet Plus"]?" *Internet Economy*, No. 4 (April 2015), p. 38.

¹⁷"China's Military Strategy," Information Office of the State Council of the PRC, May 2015, <http://www.scio.gov.cn/zfbps/32832/Document/1435514/1435514.htm>.

Department of Economic and Social Affairs ranks China 70th in the E-Government Development Index. These three authoritative international parameters of cyberspace development demonstrate that China's informatization needs are still extensive. However, due to complex national conditions and huge social diversity, cybersecurity takes precedence over informatization in China in many cases, one of which is that "network security" comes before "informatization" in the Chinese name of the Central Network Security and Informatization Leading Group. In the First China-ASEAN Cyberspace Forum held on September 18, 2014, Lu Wei also pointed out in his keynote speech that

Without security, the faster development occurs, the greater the potential harm there may be; without development, there is no guarantee for security, and existing security can even be lost.¹⁸

Therefore, a balance between informatization and cybersecurity will continue to be maintained in the course of China's development.

Vital Interests and Prevailing Threats to Cybersecurity in Chinese Perception

It seems more advisable to start from the analysis of China's cybersecurity interests if we hope to gain a better understanding of cybersecurity threats that China is facing. Cybersecurity issues have been interwoven with diplomacy, trade and personal privacy, and also involve national security, public security and personal security. However, the Chinese view of cyber issues takes "a more state-centric orientation toward cybersecurity than is the case in Western democratic nations."¹⁹ Therefore, this article tries to interpret the major threats and challenges for cybersecurity as understood by the Chinese. From an overall perspective, China's vital cybersecurity interests and challenging threats can be divided into three categories:

¹⁸See Lu Wei's keynote speech at the First China-ASEAN Cyberspace Forum, Information Office of the State Council website, September 18, 2014, <http://www.scio.gov.cn/zhzc/8/5/Document/1381275/1381275.htm>.

¹⁹Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, No. 42 (2013), p. 4.

Cybersecurity Threats to Socio-Political Stability

China's strategic interests in cyberspace are subject to its general economic, social and political security, as well as the stability of the regime. By adopting its current cyberspace strategy, China intends to safeguard its political stability as a core national interest. Seen as a quintessentially Western creation, the Internet in China has the potential to become a vehicle for subversion and the spread of Western ideas and values.²⁰ China believed that the failed color revolution in Moldova in 2009 was to a large extent instigated via social media (Twitter and Facebook) mobilization by the West although poor domestic governance also took some blame. The same was true for the abortive foreign subversion in Iran in 2009 right after the general election, which was also based on the Internet and gave rise to widespread social unrest.²¹ Moreover, from the time that China embarked on the process of evolving into an industrial and information society, its old and new social contradictions have become intertwined with each other. The Chinese government finds it necessary to carry out some regulatory measures on cyberspace in order to avoid the negative impacts of public opinions undermining social and political stability.

The American Center for a New American Security once issued a report on Chinese cyberspace strategy, which indicates that China's foreign policy behavior, including its cyber activity, is driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party (CCP).²² Michael D. Swaine also pointed out that

the PRC regime places a particularly strong emphasis on the challenges posed by cyber activities that threaten existing

²⁰Nigel Inkster, "China in Cyberspace," *Survival*, Vol. 52, No. 4 (August/September 2010), p. 62.

²¹*Ibid.*, p. 63. See also similar views in Nigel Inkster, "China—Threat or Target," *Montrose Journal*, December 2010, <http://www.montroseassociates.biz/article.asp?aid=59>.

²²Amy Chang, "Warring State: China's Cybersecurity Strategy," (Washington, D.C.: Center for a New American Security, December 2014), http://www.cnas.org/sites/default/files/publications-pdf/CNAS.WarringState.Chang_report_010615.pdf.

domestic social and political norms or values as well as the sovereignty of the nation-state.²³

These observations are basically accurate. At the Sino-U.S. Strategic and Economic Dialogue in 2009, Chinese State Councilor Dai Bingguo suggested that

with regard to China's core interests, the first priority is to maintain the basic system and national security, followed by national sovereignty and territorial integrity, and then the sustained and stable development of the economy and society.²⁴

In December 2010, writing about China's core interests, State Councilor Dai further explained that core interests included

China's state system, form of government and political stability, i.e., the leadership of the Communist Party, the socialist system, the road of socialism with Chinese characteristics.²⁵

As shown in these statements, political stability is China's first and foremost consideration regarding national interests in its cyberspace strategy.

In short, the biggest threat in cyberspace in the Chinese understanding is any factor that affects its social and political stability. Any anti-government or anti-social activities in cyberspace, any dissemination of words and deeds destabilizing the society, any cyberspace activities spreading ethnic hatred and terrorism, any plotting, organization and implementation of any acts of subversion, division or sabotage, any

Maintaining political and social stability is the predominant objective of China's cyber strategy.

²³Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, No. 42 (2013), p. 3.

²⁴For Dai Bingguo's explanation of China's core national interests at the Sino-U.S. Strategic and Economic Dialogue on July 28, 2009, see <http://www.chinanews.com/gn/news/2009/07-29/1794984.shtml>.

²⁵Dai Bingguo, "Jianchi Zou Heping Fazhan Daolu [Adhering to the Road of Peaceful Development]," *Contemporary World*, No. 12 (2010), p. 7.

violent separatist or terrorist attacks aimed at China's territorial integrity and political power consolidation through the Internet, any public opinion attacks on information network that could undermine the consolidation of the Chinese regime, the stability of the political system as well as the unity and harmony of all people, along with any other equivalent acts all fall under the primary category of threats to national security. With regard to the most serious security threat, there is a special term in China, namely the "three forces" (*sangu shili*): terrorism, separatism, and extremism. The Chinese government's key concern is that unrestricted Internet access or uncontrolled information exchange might create loopholes for foreign subversion, thus posing significant threats to China's political stability.

Cyberspace Vulnerabilities and Critical Information Infrastructure Security

Information infrastructure and cyber system security is another important aspect constituting China's strategic interests in cyberspace. It is obvious that China's informatization progress has made its economic and social activities dependent on cyberspace.²⁶ Since the security of critical information infrastructure is associated with social stability and economic prosperity, security challenges threatening critical information infrastructure and network systems might not only leave the national entities vulnerable to attacks, but facilitate the activities of terrorists and other dangerous non-state actors as well.

The fact that both core network technology and critical information infrastructure are controlled by foreign countries has become a Trojan horse for China's national security. The big gap between China and Western countries in terms of core network technical capabilities could be the leading cause. China has long been relying on Western technology in terms of chips, operating systems, databases and other core technologies. The core technology, products and critical services that China adopted in important information systems and critical infrastructure are also dependent on foreign inputs. Furthermore, servers, storage devices, operating

²⁶Zhou Qi and Wang Xiaofeng, "Wangluo Anquan yu Zhongmei Xinxing Daguo Guanxi [Cybersecurity and a New Type of Major-Power Relations between China and the U.S.]," *Contemporary World*, No. 11 (2013), p. 32.

systems and databases applied in government agencies and other public sectors are mainly of foreign patents. As the China National Vulnerability Database of Information Security (CNNVD) shows, foreign open-source software and products constitute major sources of information vulnerabilities in 2014.

The revelation of NSA's "Prism" project, the "XP Exit" as well as the leakage of some classified documents have further heightened China's awareness of cybersecurity. U.S. intelligence agencies, through the "Prism" project, took advantage of the core Internet technologies in their hands and carried out big data mining in large U.S. Internet companies, thereby posing a serious threat to China's national security. On April 8, 2014, Microsoft Corporation decided to stop the vulnerability-patching service for Microsoft Windows XP system, resulting in the exposure of thousands of millions of Chinese Windows XP users to network security risks. According to certain statistics, the installed capacity in China had reached 200 million sets of XP by the end of 2014. Plenty of PCs with Windows XP system cannot upgrade to the new Win8 due to hardware reasons,²⁷ and 57 percent of the XP users have no other choice but to make do with the obsolete system.²⁸ Risky operating systems can not only harm the systems themselves, but also place entire software applications and their data security at tremendous risk.

Against this backdrop, it is not unusual to hear two buzzwords in the past years with regard to China's information infrastructure and network system security, which are "network security review" (*wangluo anquan shencha*) and "independently controllability" (*zizhu kekong*). China believes that in order to maintain the security of critical infrastructure, import censorship must be established when it comes to servers, routers, switches, storage devices and other network facilities. On May 20, 2014, the Chinese Government Procurement Network issued a "Notice on Added Tender for Information-related Equipment

²⁷"Top Ten Information Security Events in 2014," December 31, 2014, <http://www.chinahightech.com/html/1830/2014/1231/10420490.html>.

²⁸"CNNIC: Baifenzhi Wushiqi de Zhongguo XP Yonghu Jiangzai Tingzhi Fuwuhou Jixushiyong [CNNIC: 57% of Chinese XP Users Will Continue Usage after XP Service Termination]," April 3, 2014, <http://www.199it.com/archives/207167.html>.

and Compulsory Energy-saving Products Supply Agreements,” which clearly stipulated that all computer products were not allowed to install the Microsoft Windows8 system.²⁹ China’s evolving cybersecurity legislation also emphasizes the establishment of a sound system of network access licenses for telecommunications equipment, and strengthens import cybersecurity review for foreign network products and software. Meanwhile, China believes that in order to safeguard the network information security, it must vigorously foster and support domestic networking industries, increasing the import substitution rates of network products and software in key areas with a targeted and step-by-step approach.

President Xi has reiterated the need to strengthen the capability of core technology self-dependent innovation and infrastructure construction.³⁰ Mr. Ren Xianliang, Executive Deputy Director of the Cyberspace Administration of China also pointed out that mastery of independently controllable, safe and reliable Internet core technology is the key to effectively safeguard the security of network and information, and even national security.³¹ It is noteworthy that a number of Chinese government agencies have begun to take corresponding actions. In September 2014, the China Banking Regulatory Commission issued “Instructions on the Application of Safe and Controllable Information Technology.” From 2015 to 2019, the introduction of safe and controllable information technology in the banking sector and its affiliated financial institutions should have an annual increase of no less than 15 percent, and the proportion of safe and controllable information technology in the banking industry should account for more

²⁹Central Government Procurement Center of the PRC, “Guanyu Jinxing Xinxilie Xieyi Gonghuo Qiangzhi Jieneng Chanpin Buchong Zhaobiao de Tongzhi [Notice on Added Tender for Information-related Equipment and Compulsory Energy-saving Products Supply Agreements],” May 16, 2014, <http://www.zycg.gov.cn/article/show/242846>.

³⁰See President Xi Jinping’s speech at the 17th Academician Conference of the Chinese Academy of Sciences and the 12th Academician Conference of Chinese Academy of Engineering on June 9, 2014, http://news.china.com/zh_cn/domestic/945/20140610/18551375_2.html.

³¹Ren Xianliang, “Anquan shi Hulianwang Fazhan de Youli Baozhang [Security is a Powerful Safeguard for Development of the Internet],” *Xinhua News*, August 26, 2014, http://news.xinhuanet.com/info/2014-08/26/c_133584425.htm.

than 75 percent till the end of 2019.³² This is the first public document at the national level with numerical targets to support China's own information technology and product development.

International Cyber Competition and Information Security

Cyberspace information and data security is also an indispensable part of China's cyberspace interests. In a broad sense, data security is a kind of information security. Data serves as "the oil of the Internet age," which might be among the most important strategic resources in our social life, industrial competition, and power struggles. The massive amount of cyberspace information and data showcases the latest advances in science and technology, reflecting social trends and market changes, exposing signs of threats to national security, holding battlefield intelligence and military operations, as well as other important information. The capability of safeguarding national security increases in direct proportion to that of obtaining information and data. Information and data security is also linked with a country's economic competitiveness. Moreover, the West's preponderant rule-making power in terms of resources, governance and even military operations in cyberspace poses a significant challenge to China as well.

The international pressures on China in cyberspace have mounted because of the revelation of the Prism project by former NSA contractor Edward Snowden, and also due to the rapid development of new technologies. The Prism scandal has intensified the pre-existing security anxieties of many countries. Even the EU expressed concerns about the risk of technical advantages being abused. For China, 2013 presented a clear picture of national cybersecurity threats. During this year, in addition to Project Prism,

2013 marked a new peak of Chinese caution against cyber threats from overseas, triggered by Snowden's disclosures.

³²Guo Xiaoping, "Yinjianhui Fabu Yingyong Anquan Kekong Xinxi Jishu Zhidao Yijian [CBRC Releases 'Instructions on the Application of Safe and Controllable Information Technology'," *China Stock*, September 16, 2014, http://news.cnstock.com/news/sns_bwx/201409/3180153.htm.

subsequent in-depth reports of the Stuxnet virus, along with the mass demonstrations spreading from East and North Africa to South America, further supported the evidence that the country was facing challenges in cyberspace. On the other hand, the development of new technologies also serves as a stimulus to China's perception of cybersecurity. The wide application of cloud computing, big data, mobile Internet, and the Internet of Things help promote the integration of information systems, automatic control systems and various networks. While assuming a profound role in promoting and optimizing the supportive environment of social informatization, these new technologies expose China's cybersecurity to increasing systemic risks as well.

China ascribes the security threats involving network information and data to a couple of factors.³³ The first is cloud data leakage if seen from a technical viewpoint. In the process of cloud computing, data access is in an online state, and users cannot control the routes of accessing their own data. Thus, we cannot guarantee that third parties will use these data in a legal fashion. Data might be transmitted in the clouds of different countries and the storage locations of data are less easy to determine in most cases. Not only is it difficult for a nation to be aware of cross-border transmissions, but even the transmitters themselves might not be able to track the information and data. Cloud data leakage has become a widespread problem that breaches individual privacy, trade secrets of companies, as well as national sovereignty and security.

The second factor is the difference in data processing capabilities. From a realistic perspective, data is not equally open to all subjects, and a number of subjects have a variety of analytic capacity whilst others lack this capacity completely. There are three categories of subjects involved in the field of data: the one who creates the data, the one who collects the data, and the one who has the ability to analyze the data. The last subject is the least in number but has most privileges. Surely, inequality exists among countries. This kind of inequality has largely resulted from a number of countries' hegemonic positions in the global cyberspace; on the other hand, it also

³³Cai Cuihong, "Yunshidai Shuju Zhuquan Gainian Ji Qi Yunyong Qianjing [Data Sovereignty and its Application Prospects in the Cloud Era]," *Contemporary International Relations*, No. 12 (December 2013), pp. 58–65.

stems from the differences in information and data technology advancement among countries.

Third, the lag or absence of relevant data laws and the law deficiency or inconsistency among various countries lead to a risky cyberspace. To truly guarantee cyberspace information and data security at the legislative and judiciary levels, we need to study and respond to these existing challenges and threats. The first challenge might be the decentralization of behavioral capacities, which means that a number of private sectors and individuals have the ability to access and perform cross-border transfers of a large quantity of electronic data. These behaviors are often unknown to their own national authorities. The second challenge involves disputes on data using with regard to two principles in the field of traditional justice, namely, the “subject” principle (that is, using data sources or data subjects to determine the scope of the right) or “territory” principle (that is, using the geographic locations of data existence to determine the scope of the right). The third challenge is the operational difficulty arising from the problem of data quantity. Data in the cloud era is featured in many varieties and large quantities. Thus it is extremely difficult to match each internet address with the user’s physical address, making effective supervision nearly impossible. The fourth challenge is the differences in relevant national laws and regulations. The behavior of processing and transmitting data stored in different countries is subject to different legal contexts. In most cases, each country has its own policies in data control.

International Cybersecurity Cooperation: China’s Role and Barriers to Further Progress

Like many other countries in the world, China possesses a number of its own exclusive social media outlets and search engines; however, in a globalized era, it is unrealistic for China to set up a separate “intranet” in parallel with the existing global cyberspace. Just as Lu Wei’s depiction of Sino-U.S. relations in cyberspace in his speech at the Seventh Sino-U.S. Internet Forum held on December 2, 2014, cyber state-actors have formed “a community of development and a community of shared interests and shared destiny.” Facing Western accusations that Chinese hackers launched cyberattacks on U.S. government agencies and companies, the

Chinese government reiterated its firm stance against any form of cyber-attack,³⁴ citing Chinese criminal law provision that “the use of computers in the implementation of financial fraud, theft, embezzlement, misappropriation of public funds, theft of state secrets or other crimes” is illegal and should be convicted and punished. The standpoint of each country on network freedom and network sovereignty might be different; however, these countries do share interests in safeguarding network infrastructure security, fostering connectivity of international networks, combating cyberterrorism, preventing hacking and other cyber-crimes, all of which will lay a solid foundation for international cybersecurity cooperation.

What is Meant by “International Cybersecurity Cooperation”?

According to China’s official position, common security in cyberspace among various countries can be achieved in four ways: First, by jointly maintaining the security of cyber sovereignty. Each country should act on the principles prescribed in the UN Charter and universally accepted international laws and norms, respecting each other’s rights of Internet development, utilization and management, in order to build up new orders for cyber sovereignty security through peaceful interactions and mutually beneficial and win-win solutions. Second, by jointly safeguarding information security. China would like to work with other countries to strengthen cooperation in the fight against hacking, Trojans, virus spreading, and other illegal acts. Third, by jointly safeguarding privacy. The protection of personal privacy requires various cyber actors to learn from each other and enhance cooperation. Last but not least, by jointly safeguarding technical security. Technical security is the cornerstone and prerequisite of cybersecurity. Countries can share experiences on tackling problems of core technology, making efforts to eliminate technical troubles and fix security flaws.³⁵

³⁴The Chinese government has repeatedly articulated its firm stance against cyber attacks. See “Zhongguo Yiguan Fandui Renhe Xingshi de Wangluo Gongji Xingwei [China Consistently Oppose Cyber Attacks in any Form],” *Xinhua News*, October 30, 2014, <http://news.xinhuanet.com/live/2014-10/30/c.1113050398.htm>; and “Waijiaobu Huiying Mei Ruqin Zhongguo Wangluo [MOF’s Response to U.S. Hacking into Chinese Network],” *China News*, <http://www.chinanews.com/gn/2013/06-24/4963911.shtml>.

³⁵See Lu Wei’s speech at the China-ROK Internet Roundtable, *People’s Daily Online*, December 10, 2013, <http://cpc.people.com.cn/n/2013/1223/c64102-23923716.html>.

This paper proposes that countries strengthen international cooperation in cybersecurity capacity building, cybersecurity governance, cyberspace arms control, combating cyber-terrorism, and work toward a cyberspace code of conduct, which encompasses four elements. The first is sharing threat information as well as cybersecurity management experience, especially for countries like China which has the largest number of netizens, the biggest e-business market, and the manufacturing capability of quickly developing cyber facilities. The second is to promote the transparency of cybersecurity policies and strategies in all cyber state-actors. Not only can countries increase transparency by releasing relevant policy statements on a regular basis, but they can also inform and consult with each other at the embryonic stage of policy making. The third is the coordination of discourses in cyberspace internally and internationally. It is notable that the discourses on cyberwar and cyber espionage are sometimes abused with biased interpretations. The fourth is enhancing institutional building at different levels and promotion of cooperation in practical fields. This kind of cooperation can be gradually expanded from an operational level such as in the fight against cyber-crimes on a case-by-case basis. In the meantime, we should promote institutional building in terms of crisis management, arms control and other governance mechanisms.

China's Endeavors in International Cybersecurity Cooperation

In the past two years, China has shown strong willingness to push forward international cooperation in cyberspace at the bilateral, multilateral, and international levels.

At the bilateral level, China has engaged in cooperation with the United States, Russia, South Korea, the UK and other countries. On July 8, 2013, China and America agreed to set up the Sino-U.S. Cybersecurity Working Group under the framework of the Strategic Security Dialogue, and held the first session of the working group. Although the group's activities were suspended due to the prosecution of five Chinese military officers by the U.S. Department of Justice in May 2014, it is still a

Despite the widespread skepticism of the West, China has been actively engaged in international cybersecurity cooperation, especially over the past two years.

manifestation that China and the United States have created a mechanism for cybersecurity interaction. On December 2, 2014, the Seventh Sino-U.S. Internet Forum was held in Washington, D.C. Lu Wei led a Chinese delegation to the session and delivered a keynote speech. In May 2015, China and Russia entered into a cybersecurity agreement, and reached mutual understanding on no cyberattacks against each other, as well as joint research and development in cyber technology. Actually, the Sino-Russian cooperation can be traced back to the 66th United Nations General Assembly in 2011, when China, together with Russia, Tajikistan, Uzbekistan and other countries, co-sponsored an initiative for cyberspace rule-making, namely the "International Code of Conduct for Information Security." In addition, the China-ROK Internet Roundtable Conference is held regularly between China and South Korea. On September 9, 2013, the Fifth China-UK Internet Roundtable was held in London.

At the multilateral and regional levels, regional blocs, such as the BRICS, ASEAN, Shanghai Cooperation Organization, as well as other major countries in Northeast Asia and the wider Asia-Pacific region, are all exploring a variety of mechanisms for cybersecurity cooperation. At the Fourth Meeting of High Representatives for Security Issues held on December 6, 2013, in Cape Town, South Africa, a decision was made to establish the BRICS Cybersecurity Working Group to fight against cyber-crimes. At the first China-ASEAN cyberspace forum held in Nanning, China, on September 18, 2014, China, along with Burma, Indonesia, Malaysia and other ASEAN countries, launched the initiative of building a "China-ASEAN Information Port" to promote multilateral cooperation and regional development. In 2009, China and ASEAN also instituted a China-ASEAN telecommunications regulatory council under the cooperation framework for cybersecurity. The Shanghai Cooperation Organization's Regional Anti-Terrorism Structure Council (RATS), at its March 22, 2013 session in Tashkent, Uzbekistan, reached agreement on contingency plans "to combat the use or potential use of computer networks for terrorist, separatist and extremist ends." Back in 2009, in order to strengthen law enforcement cooperation, the member countries of the Shanghai Cooperation Organization also entered into an inter-governmental cooperation agreement for the protection of international information security. From July 23 to 24, 2014, the Ninth Asia-Pacific Information Security Conference (SecureAsia) was held in Beijing. The 2014 China Internet Security

Conference (ISC 2014), the most authoritative annual summit in the field of Asia-Pacific information security, was held in Beijing from September 24 to 25, 2014. From October 28 to 30, 2014, the 2014 Northeast Asia Peace and Cooperation Initiative Forum was held, with the issue of regional cybersecurity cooperation being one of its four major themes.

At the global level, China not only participates in various cybersecurity sessions and activities, but also takes the initiative to build up a series of international cooperation platforms. From December 3 to 5, 2014, China was actively engaged in the Fifth Global Cyberspace Cooperation Summit held in Berlin. Besides, China attended the Internet Corporation for Assigned Names and Numbers (ICANN) meeting held on June 23, 2014, in London. Lu Wei delivered a keynote opening address entitled "A Cyberspace Shared and Governed by All" and put forward seven recommendations. As a member of the UN Group of Governmental Experts (GGE), a body whose mandate is to study and build norms in cyberspace, China agreed in a June 2013 report released by the GGE that international law should guide state behavior in the cyber domain. In June 2014, the 68th UN General Assembly carried out the fourth review in terms of "United Nations Global Counter-Terrorism Strategy" and adopted this resolution. In accordance with the amendments proposed by China, this resolution, for the first time, included the content of combating cyber terrorism. Furthermore, China also took the initiative to hold a variety of conferences associated with the topic of cybersecurity. On June 5, 2014, China and the United Nations jointly organized the "United Nations International Symposium on Information and Cyberspace Security" in Beijing. From November 17 to 18, 2014, Chinese Ministry of Foreign Affairs organized the Symposium on the Combat against Cyber Terrorism in Beijing, and around 70 representatives from nearly 20 member states and UN agencies explored how to strengthen international cooperation, prevent and combat cyberterrorism. From November 19 to 21, 2014, the Central Leading Group for Cyberspace Affairs held the First World Internet Conference, attracting more than 1,000 participants from nearly 100 countries and regions around the world.

Obstacles for Further International Cooperation

Despite its significance, international cooperation on cybersecurity still lingers at a preliminary stage with a number of obstacles and more words

than real actions. First, each country holds different perceptions in terms of some basic cyberspace notions, such as Internet freedom and Internet sovereignty. Therefore, these countries usually have differentiated demands in the course of international cooperation. For example, the regulatory policies China implements on cyberspace are to balance security with freedom, in favor of the idea of Internet sovereignty; in contrast, the United States attaches great importance to unrestricted "Internet freedom," stressing the role of an open society in creating favorable international environment. The United States accuses China of restricting Internet freedom and tries to influence China's social and political process by supporting technologies that could nullify China's Internet censorship. In addition, each country also sets different standards on cybersecurity issues. The United States regards it legal to carry out cyber espionage for security reasons, while such actions for commercial reasons are considered illegal. However, most countries believe espionage for either of the two motivations is unacceptable. In addition, further expansion of international cooperation on cybersecurity among different countries is affected by factors like different Internet penetration rates. As for countries with low Internet penetration rate, such as Mongolia and Brunei, their willingness to participate in international cooperation is quite weak.

The international society calls for a common perception and trust-based managing institutions of cybersecurity cooperation.

Second, from the perspective of institutional building, a neutral dominant party is required for the further expansion of international cooperation and the coordination of international conflicts; however, some disputes over the role of a leading coordinator still exist. With regard to cyberspace governance, thanks to the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Action Group (IETF), the Internet Governance Forum (IGF), and other non-governmental entities, the United States and other Western countries

advocate the multi-stakeholder governance model, insist on excluding the issues like cybersecurity and cybercrime from the International Telecommunication Regulations, and oppose United Nations intervention in the management of cyberspace content and network infrastructure. China and

other emerging economies or developing countries make no objection to the diversification of the governance body. However, they do hope that international organizations like International Telecommunications Union (ITU) can be more active and constructive, advocating the establishment of a fair and reasonable cyberspace governance mechanism, under the United Nations framework, which allows a broad participation of all countries.³⁶ The United Nations also believes that

the Internet has evolved into a global public facility. International governance of the Internet should be multilateral, transparent, and democratic, with the full participation of the government, private sectors, civil society as well as international organizations.³⁷

Also, the United Nations actively encourages the ITU to assume a leading role in Internet governance. Nevertheless, these proposals from both the United Nations and China have been rejected by the U.S. government.

Third, the inadequate strategic trust among countries might be the biggest obstacle to international cybersecurity cooperation. Generally, there are three levels of strategic trust (high, medium, and low).³⁸ Among the many existing state-to-state relationships, the U.S. and China seem to have the lowest mutual trust in general. Even compared with other aspects of Sino-U.S. relations, whether economic, political or military, the strategic trust in cyberspace appears to be the lowest. As indicated by Kenneth Lieberthal, cyber is a realm in which the most hostile images each side has of the other are being reinforced.³⁹ The status quo of Sino-U.S. strategic trust in cyberspace also creates some negative impacts on the overall

³⁶Wang Xiaofeng, "Zhongmei Guanxi Zhong de Wangluo Anquan Wenti [Cybersecurity Issues in Sino-U.S. Relations]," *American Studies*, No. 3 (Autumn 2013), p. 22.

³⁷World Summit on the Information Society, "Building the Information Society: A Global Challenge in the New Millennium." (New York: United Nations, December 12, 2003), <http://www.un-documents.net/wsis-dop.htm>.

³⁸Jay B. Barney and M. H. Hanson, "Trustworthiness as a Source of Competitive Advantage," *Strategic Management Journal*, Vol. 15, Issue Supplement (Winter 1994), pp. 175–190.

³⁹Kenneth Lieberthal and Wang Jisi, "Addressing U.S.-China Strategic Distrust," John L. Thornton China Center Monograph Series No. 4 (Washington, D.C.: Brookings Institution, March 2012), p. 47.

Sino-U.S. mutual perception, which is affected by a variety of structural factors, including social systems, values, geopolitical factors, and potential conflicts between an established great power and a rising power. Especially due to its unique nature, cyberspace has become a field where distrust in Sino-U.S. strategic relations is most likely to be demonstrated and amplified.

Conclusion

Based on unique national conditions, China has its own perception on cybersecurity. Like many other governance issues in China, the protection of cybersecurity also takes a state-dominant approach, with the aim of maintaining social and political stability, information infrastructure security, and cyberspace information and data security. And major threats to cybersecurity are the “three forces” and other activities with political motivations, vulnerability of systems controlled by foreign countries, as well as a variety of international cybersecurity games.

After the Prism scandal, international cooperation on cybersecurity has entered a new era. The international consensus with respect to the need to strengthen cooperation on cybersecurity began to rise. China’s unique understanding of cybersecurity does not limit its willingness to participate in international cybersecurity cooperation. It has to be noted that China has made great efforts in promoting cybersecurity cooperation through a number of platforms at the bilateral, multilateral, regional, and global levels. China not only plays a positive role in various cybersecurity cooperation forums, but also proposes to build up a variety of platforms of communication for cyber issues. In addition, China has already reached a number of agreements or made joint statements on cybersecurity cooperation with other countries. In spite of the progress, there are still some obstacles to overcome. As a stakeholder in cyberspace, each country has the responsibility to narrow the gap of different understandings and further promote international cooperation on cybersecurity.

As President Xi pointed out, any effective cybersecurity cooperation entails mutual respect and mutual trust of all parties in the first place.⁴⁰

⁴⁰See President Xi Jinping’s message of congratulations to the First World Internet Conference, *Xinhua News*, November 19, 2014, <http://news.xinhuanet.com/live/2014-11/19/c.127228771.htm>.

Indeed, cooperation on cybersecurity has become an international trend. For the common security of the global cyberspace, every country should undertake trust-building efforts, through various means, such as respecting each other's Internet sovereignty, reaching a unified cyberspace code of conduct, identifying the common threats to cybersecurity, establishing a sharing mechanism for network threat information, putting hotlines in operation, and concluding bilateral or multilateral agreements. In doing so, possible misjudgment, occasional conflicts or cyber warfare at the expense of national security and global network information system may be averted. With all these efforts, the prospect of a peaceful, secure, open, and cooperative cyberspace will be more promising.