SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Konrad Adenauer Stiftung

9th Berlin Conference on Asian Security (BCAS)

International Dimensions of National (In)Security
Concepts, Challenges and Ways Forward

Berlin, June 14-16, 2015

A conference jointly organized by Stiftung Wissenschaft und Politik (SWP), Berlin and Konrad-Adenauer-Stiftung (KAS), Berlin

Discussion Paper
Do Not Cite or Quote without Author's Permission

Session III: Cyber Security

Cuihong Cai
Center for American Studies, Fudan University
Shanghai

Cybersecurity in Chinese Context: Changing Concepts, Vital Interests and Cooperative Willingness

Cuihong Cai

Abstract: "Cybersecurity" has been upgraded to a major strategic topic concerning both national security and international security, especially after Edward Snowden's disclosure of the secret surveillance programs of the US government. As a country with the biggest number of netizens, China is no exception. To understand the challenges and opportunities presented to international cooperation on cybersecurity, it is important to examine in some detail the Chinese views, beliefs, and apparent assumptions toward the subject. This article addresses Chinese thinking on three aspects of the issue: China's views and perceptions of cyberspace and cybersecurity in general, the vital cybersecurity interests and threatening challenges in Chinese understanding, and China's role in international cybersecurity cooperation and barriers to progress.

Key Words: cybersecurity, cyberspace, China, information security

Introduction

Many of China's recent moves regarding cybersecurity are indicative of the issue's growing significance attached to cybersecurity. Most notably, the Central Network Security and Informatization Leading Group was established in February 2014.[1] President Xi Jinping, acting personally as the group leader, proposed a critical thesis of "No cybersecurity, no national security; no informatization, no modernization". Xi Jinping's remarks at the first session demonstrated the importance of cybersecurity on the Chinese political agenda and signaled a new, high-level prioritization of cyber as a major strategic initiative with political, economic, and military implications. Lu Wei, the Deputy Minister of the Propaganda Department of the Central Committee of the CPC, the Director of the Office of the Central Network Security and Informatization Leading Group and the Director of the Office of the National Leading Group for Cyberspace Affairs, delivered the keynote speech in the Second China-ROK Internet Roundtable Conference held on Dec. 10, 2013. At that meeting, he also pointed out, "Security is important. Security has gone beyond the scope of technology, with more

[1] President Xi Jinping's speech at the first session of Central Network Security and Informatization Leading Group, Feb. 27, 2014 , http://www.cac.gov.cn/2014/02/27/c_133148354.htm.

decisive significance. Security entails innovation, protects development and leads technology. It is the forerunner of the market as well as the symbol of core competitiveness. The one who controls the "lifeline" of security is ahead of the game, thereby standing out in the course of the next generation Internet development.[2]" In addition to the official statements concerning cybersecurity, many additional measures taken by China in the past two years also illustrate this point. For example, China's First National Cybersecurity Week was successfully held from Nov. 24 to Nov. 30, 2014, and the second one was just held from June 1 to June 6, 2015, both aimed to promote nation-wide cybersecurity consciousness.

China's Views on Cyberspace & Cybersecurity in General

Distinctive national conditions in China give rise to a difference in the perceptions of cybersecurity between China and western societies, in both the choice of words, or in the different perspectives on cybersecurity. In China's case, cybersecurity is more than an issue of technical security and safeguards, but an issue of social governance and security.

1. *Changing Concepts from Information Security to Network Security and Cybersecurity*

Corresponding to the word "cyber" used by the western societies, China adopts the word "network". "Cyberspace" is usually referred to as "network space" in the literal translation of Chinese, and is sometimes also transliterated as Saibo space in Chinese Pinyin. In Chinese, Internet Security, Network Security as well as Cyber Security share the same wording as cybersecurity（网络安全, wangluo anquan）. Chinese media, policy makers and researchers are still struggling with the conclusive choices of words for cybersecurity and related terms. It is difficult for the word "cybersecurity" to achieve complete equivalence in Chinese language, and there is no official definition with respect to the concept of "cybersecurity" although the draft Cybersecurity Law is planning to make it clear. Currently, Chinese writers usually adopt two associated words, namely "information security" (信息安全， xinxi anquan)and "network security" （网络安全, wangluo anquan）. "Network security" is often translated as Cyber Security in English. Even though Chinese scholars have in recent years gradually aligned with the West in choice of words, we must still elaborate the distinction between the two phrases.

[2] Lu Wei's keynote speech at China-ROK Internet Roundtable Conference, Dec. 10, 2013, http://news.xinhuanet.com/world/2013-12/10/c_118489322.htm.

The choice of words has been in constant development and undergone many changes. And in the early eras of communication confidentiality and stand-alone computers, the common expressions for security issues were “communications security”, and “computer security”. “China’s Computer Management Ordinance”, issued by the State Council in 1994, employed the phrase of “computer security”. With the rise of the Internet, the terms for information and network security began to show diversification. But later on, the understanding gradually came to be unified and the phrase, “information security”, was adopted as the exclusive term for this line of business, and is consistently used in a variety of official documents. After the establishment of Office for National Leading Group for Cyberspace Affairs, in the official context, there was a period of time when internet content management belonged to the scope of information security while internet technology management belonged to the scope of network security, in order to differentiate their focus of their work from that of the Ministry of Industry and Information Technology. Nevertheless, the media and the academia still regard “information security” as the mainstream term.[3] Today, in order to comply with the developing trend of international cyberspace security and to echo the language of the Western, English-speaking world, the official documents in 2014 began to frequently adopt the term “cybersecurity”, slightly different with the previously used term “information security”. However, sometimes official documents still retain the term “information security”, and the perception of “information security” may remain for a longer time in the academic community and the military. For example, in the document of “Instructions on Further Strengthening Military Information Security”, issued by the Central Military Commission and approved by President Xi Jinping in October 2014, the term “information security” was still used. Also, the term, “information security”, appeared in 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” is more focused on data information in the network, which is usually referred as “content”. Each of the terms stresses different aspects. Traditionally, China prefers to use the concept of Information Security, which is viewed essentially from the perspective of maintaining ideological security, with an emphasis on the nation’s control and dominant power over information flow. During Lu Wei’s speech at the China-ROK Internet Roundtable Conference on Dec. 10, 2013, he mentioned that “Information is the

[3] Cui Guangyao, “Information security, Impression 2014,” China Information Security, No.1, 2015, p.51. (崔光耀:“信息安全·印象 2014”,《中国信息安全》， 2015 年 1 期,第 51 页。).

'blood' of the Internet. The Internet will be lifeless without the security of information content."[4]

Even the notion of cybersecurity has also been evolving in the recent two years. The previous term for cybersecurity, better interpreted as network security, was mostly a purely technical term; while the same term, cybersecurity, now includes not only technology, but also human behaviors as well as the relationship between different actors.. That is to say, cybersecurity has transcended the scope of strictly technology. It not merely refers to the security of network hardware, network information and cybersecurity software, but also indicates the orderliness of human activities in the cyberspace society. In a 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, reliable with normal operations, and network services are without any interruption. From the perspective of orderliness, cybersecurity indicates an orderly fashion in which people are able to carry out a variety of activities in cyberspace. These two types of security are inextricably linked and mutually reinforced. 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.

2. Network Sovereignty and Cybersecurity under the "Holistic National Security Outlook"

Since 2014, "Holistic National Security Outlook" (总体国家安全观, zongti guojia anquan guan) serves as the guiding principles of national security for the Chinese government. On January 24, 2014, National Security Commission of the Communist Party of China was established to coordinate the major issues and high-priority work related to national security. On April 15, President Xi Jinping chaired its first session and stressed the need to accurately grasp the new features and new trends concerning any changes in national security situations, to adhere to the Holistic National Security Outlook, and to take a path of national security with Chinese characteristics. He also pointed out the demands to build up a national security system encompassing political security, homeland security, military security, economic security, cultural security, society security, science and technology security, information security, ecological security, resource security as well as nuclear security. President Xi Jinping

[4] Lu Wei's speech at the China-ROK Internet Roundtable Conference, Dec. 10, 2013, http://news.xinhuanet.com/world/2013-12/10/c_118489322.htm.

summarized the "Holistic National Security Outlook" with 71 Chinese words, which is translated in 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."[5]

Clearly, cybersecurity is closely linked to almost every aspect of China's national security system. Cyberspace is a complex that runs through a multi-dimensional space-time field, integrates complicated internal and external factors and covers both the connotation and denotation of the security issue. Network is the basic structure of the overall systems and national security issues have become a "network mixture". Clearly, cyberspace has turned into the strategic cornerstone of national security in the Internet age. The security issues appearing in the domains of the land, the sea and the air are all under the direct control of cyberspace. Thus, various kinds of national security issues are subject to cyberspace communication. Also, cyberspace is the domain where new situations, new problems, new features and new trends are expressed in most cases. Xi Jinping's statement of "no cybersecurity, no national security" indicates the intrinsic links between cyber security and national security in various "domains".

At the same time, based on the Holistic National Security Outlook, along with China's basic national conditions, China's stance on the issue of cyberspace is as follows: by identifying with the idea that international interconnection and interworking are the premise of sustainable cyberspace development, China hopes to clarify the relations between cyberspace and national sovereignty, as per "The Chinese government believes that the Internet belongs to critical national infrastructure, that the Internet within the territory of the People's Republic of China is under the jurisdiction of Chinese sovereignty, and that China's Internet sovereignty shall be respected and protected."[6] China is in favor of the international consensus that "the decision-making power of Internet-related public policy issues should be a matter of national sovereignty", but China does not insist that sovereignty should cover all matters in cyberspace. Meanwhile, China is opposed to absolute network security, believing that "there are no double standards in the field of information. Every country is entitled to maintain its own information security. It is not allowed

[5] President Xi Jinping's speech at the first session of National Security Commission of the Communist Party of China: "Adhere to the Holistic National Security Outlook, and take a path of national security with Chinese characteristics"（"坚持总体国家安全观，走中国特色国家安全道路"）, April 15, 2014, http://politics.people.com.cn/n/2014/0416/c1024-24900227.html.

[6] The Information Office of the State Council of PRC: The Internet in China《中国互联网状况》, Beijing: People's Publishing House, 2010 edition, p. 20.

that one nation is secure while others are insecure, nor one part of the nation is secure while the other parts are insecure. No nation shall seek its own alleged absolute security at the expense of other countries' security."[7]

Thus, in the message of congratulation for the first World Internet Conference held on Nov. 19, 2014, President Xi Jinping also placed the significance of respecting network sovereignty before that of maintaining network security.[8] He stated that "China is willing to deepen the international cooperation with other countries, to respect network sovereignty, and to maintain network security." In the China-ROK Internet Roundtable Conference held on Dec. 10, 2013, Lu Wei put forward four proposals, among which, the first one 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, and that information service is able to transcend national borders, but that cyberspace cannot exist without sovereignty. Based on the purposes and principles of UN Charter as well as the accepted norms of international law, we shall respect each nation's rights of Internet development, utilization and management, oppose network hegemony, and actively build new orders of network sovereignty security, with peaceful coexistence and win-win mutual benefit.[9] Besides, in the First China-ASEAN cyberspace forum held on Sep. 18, 2014, Lu Wei also noted in his keynote speech that "the cyberspace should be interconnected, and meanwhile be respectful of sovereignty. Information dissemination has no national borders, but cyberspace does have boundaries. We have to respect the network sovereignty of each country and ensure every country's sovereignty and interests in the field of information by avoiding any violation."[10]

3. Informatization and Cybersecurity under the Guiding Goal of "Cyberpower"

After the Central Network Security and Informatization Leading Group was established in February 2014, President Xi Jinping put forward the strategic goal of becoming a Cyberpower (网络强国，wangluo qiangguo). This goal includes two aims. One is to hope to become a major power in cyberspace, and the other is to improve national power through networks. What is a cyberpower? This is a new

---

[7] President Xi Jinping's speech at the Brazilian Congress: Carry forward the traditional friendship and jointly compose a new chapter , http://news.sina.com.cn/c/2014-07-18/184230543560.shtml.

[8] President Xi Jinping's message of congratulation for the first World Internet Conference, Nov. 19, 2014, http://news.xinhuanet.com/live/2014-11/19/c_127228771.htm.

[9] Lu Wei's speech at the China-ROK Internet Roundtable Conference, Dec. 10, 2013, http://news.xinhuanet.com/world/2013-12/10/c_118489322.htm.

[10] Lu Wei's keynote speech in the First China - ASEAN Cyberspace Forum, Sep. 18, 2014, http://www.scio.gov.cn/zhzc/8/5/Document/1381275/1381275.htm.

concept. In general terms, cyberpower is marked as "The Internet industry possesses strong global competitiveness. Major national infrastructure has complete defense capabilities. Network security and military fields possess adequate deterrence."[11] I personally believe that the China's alleged "cyberpower" does not mean that China will impose its own cyberspace doctrine upon others, but means that their own cyberspace capabilities should be strong enough to be self-sufficient, without the need to depend on others. This goal responds to the current circumstance where Chinese cyberspace possesses a wealth of infrastructure but is still dependent on foreign products. Meanwhile, the proposed target is also based on China's current status as an Internet power. From the perspective of the number of Internet users, both China's Internet users and mobile users rank first in the world. Furthermore, China has already built up a 4G network and has the largest user base around the world.

Cyberpower goals include two main lines of work: informatization and cybersecurity. China attaches equal importance to both of these aspects. Cybersecurity and informatization are considered as "two wings on one plane, two wheels on one motorcycle", and they must be under unified planning, unified deployment, unified propulsion and uniform implementation. In the first session of Central Network Security and Informatization Leading Group, President Xi Jinping proposed the strategic goal of building up cyberpower and pointed out: "A slight move in cybersecurity and informatization may affect a country's various areas as a whole. No cybersecurity, no national security. No informatization, no modernization. Good performance in cybersecurity and informatization depends on the proper handling of the relations between security and development, as well as coordination and side-by-side advancement. Only by using security to guarantee development and using development to promote security, can long-term peace and order be realized."[12]

China is fully aware that the legitimacy of the Chinese political party does not rely on ideology, but on its economic and social development. Therefore, in the process of regulating cyberspace for the purpose of protecting social stability, China does not want to jeopardize its economic and social development. From this point of view, China's policy could be interpreted as fundamentally pragmatic.. Network development and informatization are conducive to social and economic development, and thereby are helpful for the improvement of political legitimacy. The sayings "Development is the largest security, while development is also the biggest politics"

---

[11] Fang Xingdong, Hu Huailiang, Cyberpower: The Great Game of China-US in Cyberspace, Publishing House of Electronic Industry, Preface, p. IX.（方兴东、胡怀亮：《网络强国：中美网络空间大博弈》, 电子工业出版社，序言第 IX 页。）.

[12] President Xi Jinping's speech in the first session of Central Network Security and Informatization Leading Group, February 27, 2014, http://www.cac.gov.cn/2014-02/27/c_133148354.htm.

also originate therefrom. The “Internet+” perception is China’s recent nationwide hot issue and is written into the Report on the Work of the Government, which is a major policy preference whereby the government expects to further promote economic and social development via leverage of the Internet. “Internet+”, based on the Internet platform, “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.”[13]

In addition, the military application of informatization is also an essential safeguard for cybersecurity. In the White Paper on China’s Military Strategy published by the Information Office of the State Council in May, 2015，Cyberspace is defined as a new pillar of economic and social development, and 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.”[14]

The road ahead of China’s informatization will be long. According to the average quality of cyberspace development, China considers itself to be one of the developing countries in general. As indicated by the “Measuring the Information Society Report 2014” issued by the International Telecommunication Union in 2014, China’s Information Development Index (IDI) ranks 86th in the world; "Global Information Technology Report” from World Economic Forum in 2014 shows that China Network Readiness Index (NRI) ranks 62th globally. "Global E-Government Survey 2014" issued by United Nation Department of Economic and Social Affairs demonstrates that China’s E-Government Development Index ranks 70th worldwide. These three authoritative international measures of cyberspace development demonstrates that China’s overall network quality still belongs to the level of the developing countries, and its informatization needs are still extensive. But in fact, because of China’s complex national conditions and huge social diversity, cybersecurity is placed before informatization in many cases. Likewise, in the Chinese name of Central Network Security and Informatization Leading Group, network security is put ahead of

---

[13] Si Xiao et al, “What is ‘Internet +’?”, Internet Economy, No. 4, 2015, p. 38（司晓等：“‘互联网+’是什么？”, 《互联网经济》, 2015 年第 4 期, 第 38 页。）.

[14] The White Paper on China’s Military Strategy（《中国的军事战略》白皮书）, published by the Information Office of the State Council in May, 2015, in part IV (Building and Development of China’s Armed Forces), http://www.fmprc.gov.cn/ce/cebe/chn/bps/t1266971.htm.

informatization, which seems to indicate its priority. In the First China-ASEAN cyberspace forum held on Sep. 18, 2014, Lu Wei also pointed out in his keynote speech: "We need to accelerate the development pace of cyberspace, but also to ensure its security. Without security, the faster development occurs, the greater the potential harm may be; without development, there is no guarantee for security, and existing security can even be lost."[15] Therefore, informatization and cybersecurity will continue to have a balanced relationship in the course of China's development.

Vital Cybersecurity Interests and Challenging Threats in Chinese Understanding

In international security studies, threats and interests are closely related. Therefore, the analysis of China's cybersecurity threats must firstly start from the analysis of China's cybersecurity interests. The understanding of cybersecurity changes with security threats and challenges in a dynamic way. Cybersecurity issues have gone far beyond the scope of technical security and system protection, and evolved into an integrated security issue concerning political, economic, cultural, social, military and other fields. Increasingly, cybersecurity issues have been interwoven with diplomacy, trade, and personal privacy, and have involved national security, public security and personal security at all levels. Although this article mainly focuses on cybersecurity issues at a national and societal level, certainly, personal cybersecurity cannot be ignored. Many major events concerning Chinese personal information security have occurred recently. Black markets for the illegal acquisition, theft, trafficking and utilization of online personal information continue to grow, becoming businesses, and involving international transactions and intelligence. However, Chinese views take "a more state-centric orientation toward cybersecurity than is the case in Western democratic nations."[16] Therefore, this article will interpret the major cybersecurity threats and challenges in China's understanding from the overall perspective of the country. China's vital cybersecurity interests and threats can be divided into the following three categories:

[15] Lu Wei's keynote speech in the First China - ASEAN Cyberspace Forum, Sep. 18, 2014, http://www.scio.gov.cn/zhzc/8/5/Document/1381275/1381275.htm.

[16] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," China Leadership Monitor, No. 42, 2013, p.4.

1. Political Cybersecurity Threats and Interest of Social and Political Stability

China's strategic interests in cyberspace are subject to general economic, social and political security as well as the stability of the regime in China. And the pursuit of political stability can be seen as a core interest of China's current cyberspace strategy. For China, the Internet, seen as a quintessentially Western creation, holds many terrors as a vehicle for subversion and the spread of Western ideas and values.[17] China believed that the failed color revolution in Moldova in 2009 was largely instigated via Twitter and Facebook although internal factors could not be ignored. The same was true of the period following Iran's 2009 election when foreign subversion from the Internet gave rise to widespread social unrest.[18] Moreover, China is in its transition to an industrial and information society. During this process, the old and new social contradictions have become intertwined. In order to achieve this aim, the Chinese government needs to avoid the negative impacts of public cyberspace opinions on social and political stability, and to carry out proper regulation of the network.

The American Center for a New American Security 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).[19] American scholar 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 domestic social and political norms or values (such as the dissemination of false rumors) as well as the sovereignty of the nation-state."[20] These observations are basically accurate. At the Sino-US 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 thirdly the sustained and stable development of the economy and society."[21] In Dec. 2010, he also wrote an article entitled "Adhere to the road of peaceful development" and pointed out China's core interests, with the first priority in

---

[17] Nigel Inkster, "China in Cyberspace," Survival: Global Politics and Strategy, Vol.52, No.4, 2010, p.62.

[18] Ibid., p.63. Similar statement is also available at: Nigel Inkster, "China - Threat or Target", Montrose Journal, Dec. 2010, http://www.montroseassociates.biz/article.asp?aid=59.

[19] Amy Chang, Warring State: China's Cybersecurity Strategy, Dec. 2014, released by Center for a New American Security, http://www.cnas.org/chinas-cybersecurity-strategy.

[20] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," China Leadership Monitor, No. 42, 2013, p.3.

[21] Dai Bingguo's explanation of China's core national interest in Sino-US Strategic and Economic Dialogue on July 28, 2009, available at http://www.chinanews.com/gn/news/2009/07-29/1794984.shtml.

more detail as “China’s state system, form of government and political stability, that is to say, the leadership of the Communist Party, the socialist system, the road of socialism with Chinese characteristics respectively”.[22]As show in these statements, political stability is China’s first and foremost consideration regarding national interests in its cyberspace strategy.

Thus, in China’s case, the biggest threat of cyberspace is any factor that affects its social and political stability. Any anti-government or anti-social activities through the cyberspace, any dissemination of words and deeds destabilizing the society, any cyberspace activities inciting ethnic hatred and terrorism, any planning, organization and implementation of any acts of subversion, division or sabotage, any violent separatist terror attacks aimed at China’s territorial integrity and political power consolidation through the network, 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 peoples, along with any other equivalent acts all fall into the primary category of threats to national security.

With regard to the most serious political threat, China has a special term, namely the “three forces” (三股势力，sangu shili) which are terrorists, separatists and extremists. The Chinese government worries that unrestricted Internet access or uncontrolled information or dissent might become a tool of subversion and pose a significant threat to Chinese political security. “Three forces” activities may come from national entities or non-national entities. Non-government organizations, companies that have a dominant position in the field of information and communication technology, transnational cyberspace activists and other non-national entities possess increasingly strong capabilities to challenge the sovereignty of a country. Therefore, while the United States cyberspace surveillance focuses on privacy, cyber-crime, terrorism and the like, China carries out tighter regulations in terms of political information as well as any information that may jeopardize social stability in addition to the domains that United States policy focuses on.

2. Cyberspace System Vulnerabilities and Interest of Critical Information Infrastructure Security

Information infrastructure and cyberspace system security represent another important national interest of China. With the rapid development of the informatization process, China has entered a stage where both economic operations and social operation depend on cyberspace; therefore, the major focal points for ensuring network security

[22] Dai Bingguo, “Adhere to the road of peaceful development", Contemporary World, No.12, 2010, p.7.（戴秉国：“坚持走和平发展道路”，《当代世界》，2010 年第 12 期，第 7 页。）.

have included the protection of information infrastructure, the safeguard of network systems, and especially the security of the critical information systems related to people's livelihood.[23] The security of critical information infrastructure is associated with the vital interests of national stability, the economy, and every individual citizen. Critical infrastructure is defined in the US as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or security, or any combination of those matters."[24] China adopts a similar definition of critical infrastructure. The security threats towards critical information infrastructure and network systems may not only leave the national entities vulnerable to attack, but also facilitate terrorists and other non-national actors.

The circumstance where both core network technology and critical information infrastructure are controlled by others has become a weakness for national network security, like a huge sword of Damocles hanging above China's head but held by other countries. There is still a big gap between the core network technical capabilities of China and that of Western countries. 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 adopted in important information systems and critical infrastructure are also dependent on foreign inputs. Furthermore, servers, storage devices, operating systems and databases applied in government departments and important sectors are mainly of foreign patents. As the China National Vulnerability Database of Information Security (CNNVD) shows, the information security vulnerabilities in 2014 mainly come from foreign open-source softwares and foreign products.

Revelations such as the NSA's "XP Exit" and "Prism" programs as well as the exposure of classified documents have heightened China's awareness of information infrastructure and cybersecurity. US intelligence agencies, through the "Prism" project, took advantage of the core Internet technologies in their hand to create a "back door" in network hardware, and carried out big data mining in large Internet companies of the United States, thereby posing a serious threat to China's national security. On April 8, 2014, Microsoft decided to stop the patch vulnerabilities service for Microsoft Windows XP system, resulting in a majority of systems of Chinese government and industry users being exposed to network security risks. According to

---

[23] Zhou Qi and Wang Xiaofeng, "Cybersecurity and New Sino-US relations Between Big Powers," Contemporary World, No. 11, 2013, p.32.（周琪、汪晓风："网络安全与中美新型大国关系"，《当代世界》，2013 年第 11 期，第 32 页。）.

[24] Framework for Improving Critical Infrastructure Cybersecurity, released by National Institute of Standards and Technology on Feb.12, 2014, p.3, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

statistics, by the end of 2014, the installed capacity in China reached 200 million sets of XP. Plenty of machines cannot upgrade to Win8 due to hardware reasons,[25] of which, 57% of the system users still continue to use XP after XP stopped its service.[26] The operating system is the "shortcut" and "main channel" for hackers to carry out their acts of sabotage and theft. Risky operating systems can not only harm the systems themselves, but also pose certain threats to entire software applications and data security programs based upon them.

Therefore, it is easy to understand two buzz words with regard to China's information infrastructure and network systems security in the past two years, which are "network security review" (网络安全审查,wangluo anquan shencha) and "independently controllability" (自主可控, 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 of added tender for information-related equipment and compulsory energy-saving products supplied agreements", which clearly stipulated that all computer products were not allowed to install US Microsoft Windows 8.[27] In addition, Symantec software was also disabled among Public Security Department due to back door information thefts. China's evolving cybersecurity legislation places the improvement of network infrastructure protection on the priority list as well, stresses the establishment of a sound system of network access licenses for telecommunications equipment, and strengthens import cybersecurity safeguards for foreign network products and software. Meanwhile, China believes that, in order to safeguard the network information security fundamentally, it must vigorously foster and support the domestic networking industries, promote the development of network products and software with their own intellectual property rights pursuant to applicable law, increase the import substitution rates of network products and software in key areas with a targeted and step-by-step approach, and further develop independently controllable network products and software.

Thus, President Xi Jinping pointed out the need to strengthen core technology self-dependent innovation and infrastructure construction, and to improve the capacity of information collection, processing, dissemination and utilization. "We cannot always

---

[25] "Top ten Information Security events in 2014", http://www.chinahightech.com/html/1830/2014/1231/10420490.html.

[26] "CNNIC : 57% of the Chinese XP users will continue to use after XP stopped its service", http://www.199it.com/archives/207167.html.

[27] "Notice of added tender for information-related equipment and compulsory energy-saving products supplied agreements" (关于进行信息类协议供货强制节能产品补充招标的通知), http://www.zycg.gov.cn/article/show/242846.

decorate our own tomorrows by virtue of someone else's yesterdays, nor expect to rely on scientific and technological achievements of others to improve our own technological levels. What's more, we cannot subordinate ourselves to other countries' technology nor always imitate someone else at every step." [28] Ren Xianliang, the Deputy Director of the State Internet Information Office 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, even national security.[29] Some related organizations have begun their implementation. In Sep. 2014, China Banking Regulatory Commission issued "Instructions on the application of safe and controllable information technology". From 2015 onwards, the introduction of safe and controllable information technology in banking financial institutions should annually increase at no less than 15% until the year of 2019, when the core knowledge and key technologies of the banking industry informatization are under national control, and the proportion of safe and controllable information technology in the banking industry reaches no less than 75% of the total.[30] This is the first national-level public document with numerical targets setting, in the aspect of supporting China's own information technology and product development.

3. The International Cybersecurity Competition and Interest of Information and Data Security

Likewise, cyberspace information and data security are also core interests that China demands in the field of cyberspace. Data serves as "the oil of the Internet age", which is the most important strategic resource in the future of social life, industrial competition and the struggle between great powers. A large quantity of cyberspace data from the Chinese government, business enterprises and users involves national interests; however, China is still faced with the lack of legal basis, technical approaches and other issues when it comes to safeguarding the interests of data security. Therefore, cyberspace monitoring, cyberspace attacks, cyberspace deterrence, cyberspace theft and other international cybersecurity conflicts related to

---

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

[29] Ren Xianliang, "Security is a strong guarantee for the development of the Internet"（任贤良："安全是互联网发展的有力保障"）, August 26, 2014, http://news.xinhuanet.com/info/2014-08/26/c_133584425.htm.

[30] China Banking Regulatory Commission issued "Instructions on the application of safe and controllable information technology" in Sep. 2014, available at http://news.cnstock.com/news/sns_bwkx/201409/3180153.htm.

information and data are all the challenges confronting China. This massive amount of cyberspace information and data contains the latest science and technology, social trends, market changes, signs of threats to national security, battlefield intelligence and military operations as well as other important information. From the perspective of national security, the capability to obtain information and data is in direct proportion to the capability of maintaining national security and the capability of defense deterrence. From the perspective of economy, information and data security is also linked with a country's economic competitiveness. From the perspective of diplomacy, domination of rule formulation in terms of resources, governance and even military operations in cyberspace poses a significant challenge to China as well.

The international cybersecurity pressures that China is confronted with have two main stimulating factors: the Prism events revealed by Snowden as well as the rapid development of new technology. The publication of Project Prism has triggered the pre-existing security anxiety of each country. The negative reactions it arouses are far beyond any previous similar events, which spark huge concerns of other countries, including the EU, about the United States' ability to abuse their technical advantages. After the Prism event, no country can say that they are not up against the competition in cyberspace, and national security is faced with a brand new competitive dimension and threat sources. For China, 2013 is the starting year when national cybersecurity threats have become clearer. During this year, in addition to Project Prism, subsequent in-depth reports about the Stuxnet virus, as well as the mass demonstrations spreading from East and North Africa to South America, were further evidence that the country was facing a huge challenge in cyberspace. This kind of challenge included not only the technical dimensions, but also the institutional and policy aspects; both real and material, as well as psychological and cognitive factors. More and more countries begin to realize the urgency, significance and inevitability of the cyberspace security challenge. Furthermore, the development of new technology is another stimulus that China has perceived in this field. The development and application in the aspects of cloud computing, big data, mobile Internet and the Internet of Things help promote the integrated development of information systems, automatic control systems and various networks. The previous network is relatively independent and decentralized, but is now comprehensively integrated with depth correlation and mutual dependence. While assuming a profound role in promoting and optimizing the supportive environment of social informatization, these new technologies expose our cyberspace to increased systemic risks as well, with growing competitive pressure from cybersecurity.

For China, the security threats to network information and data are derived from a couple of factors.[31] The first one is, from a technical point, the problem of cloud data leakage. 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, it cannot be guaranteed whether third parties will misuse the data or not. Data may be transmitted in the clouds of different countries, and the storage locations of data are difficult to determine in most cases. Not only is it difficult for a nation to be aware of cross-border transmission, but even the transmitters themselves may not track the information and data. The problem of cloud data leakage has become widespread and poses a serious threat to the privacy of individuals, trade secrets of corporations as well as the sovereignty and security of any nation.

The second factor is the difference in data processing capabilities. In fact, data is not open to all subjects equally, and a number of subjects do not have the analytical capacity or have different capacities of analysis. 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 of the least number but with the most privileges, and furthermore, they are the protagonists who decide the rules for big data. Surely, there is inequality between countries. This type of inequality is resulted from a number of countries' hegemonic position in the global cyberspace; on the other hand, it also stems from the differences in information and data technology levels between the countries.

The third factor is the lag or absence of relevant data laws as well as inconsistencies among various countries from the perspective of law. To truly implement cyberspace information and data security in the operational levels of legislative, judicial and enforcement, there are still many challenges we need to study and respond to together. The first one is the decentralization of behavioral capacities, where a number of private sectors and even individuals have the ability to access and perform cross-border transfers of a large quantity of electronic data. And their behavior is often unknown to their own national authorities. The second one involves the disputes in the field of data regarding the "subjects" 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) in the field of traditional justice. The third one is the practical operational difficulty arising from the problem of data quantity. Data in the cloud era is featured in many varieties and large quantities, and what is more, the Internet addresses and

[31] Cai Cuihong, "Data Sovereignty and Its Application Prospects in the Cloud Era," Contemporary International Relations, No. 12, 2013, pp. 58-65.（蔡翠红："云时代数据主权概念及其运用前景"，《现代国际关系》，2013 年第 12 期，第 58-65 页。）.

physical addresses cannot achieve one to one correspondence. The fourth one is the differences in relevant national laws and policies. The acts of processing and transmitting data stored in different countries are subject to different legal regulations in different countries. In most cases, each country holds different policies in the aspect of data, which poses a critical national security threat. For example, the foreign companies which operate Internet business in the territory of China get hold of a data base belonging to Chinese Internet users. If these foreign companies submit the data and information in their systems to the home country government pursuant to home country law, China's national interests and national security will be under threat.

China's Role in International Cybersecurity Cooperation and Progress Barriers

Cyberspace is interconnecting the whole globe, which puts forward new challenges to national sovereignty, security and development interests. Each country must positively participate in international competition, and take an active involvement in international cyberspace cooperation. China, in the eyes of many other countries, possesses a number of its own exclusive social networks and search engines; however, in a global networked era, clearly, China is not likely to set up separate networks which are entirely parallel to the existing global cyberspace. The cybersecurity that China pursues is still one in an open environment, rather than fragmented or LAN-based cybersecurity. Just as Lu Wei's description of Sino-US relations in the cyberspace in his speech at 7th Sino-US Internet Forum held on Dec. 2, 2014, the countries in current cyberspace have become "a community of development, a community of interests and a community of destiny." Regarding the Chinese hacking accusations by the foreign media, not only Chinese officials have repeatedly stated "the Chinese government has always been opposed to any form of network attack behavior," 32Chinese criminal law also clearly stipulates in article 287 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. Each country's views toward network freedom and network sovereignty may be different, however, the countries share common interests in the aspects of safeguarding network infrastructure security, maintaining the connectivity of international networks, combating cyberterrorism,

[32] This statement was made clearly and formally on many occasions. Available at http://news.xinhuanet.com/live/2014-10/30/c_1113050398.htm; http://www.chinanews.com/gn/2013/06-24/4963911.shtml.

opposing hackers and other cyber-crimes, all of which lay an important foundation for international cybersecurity cooperation.

1. Contents of International Cybersecurity Cooperation

According to China's official language, the joint maintenance of cyberspace security between various countries can be carried out in four ways: The first one is to jointly maintain the security of network sovereignty. Each country should proceed from the principles of the "UN Charter" and from the prevailing international laws and norms, respect each country's various rights of Internet development, utilization and management, oppose network hegemony, and actively build up new orders for network sovereignty security with peaceful coexistence, mutual benefit and win-win scenarios. The second aspect is to jointly safeguard information security. China hopes to unite more countries in the course of strengthening the cooperation of cyberspace information security and jointly fighting against hacker attacks, trojans, virus spreading and other illegal acts. The third one is to jointly safeguard privacy. The protection of personal privacy requires that countries learn from each other, enhance cooperation, and effectively increase the protection of individual information. The fourth one is to jointly safeguard technical security. Technical security is the cornerstone and the prerequisite of cybersecurity. Countries can share experiences with each other, jointly help to tackle problems of core technology, key equipment, mobile terminals and other aspects, make efforts to eliminate technical troubles, fix security flaws, and support cyberspace development with excellent technology and reliable systems.[33]

From my personal point of view, countries can carry out international cooperation in the field of security capacity building, cybersecurity governance, cyberspace arms control, cyber-terrorism and a cyberspace code of conduct. They can be divided into four areas. The first one is sharing their threats information as well as cybersecurity management experience, especially for a country like China which has the largest number of cyber 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 countries. Not only can countries demonstrate their transparency after the publication of policies, they can also inform and consult with each other at the embryonic stage of the policy development. The third way is the coordination of narratives in cyberspace internally and internationally. For example, the narratives on cyberwar and cyber espionage are

[33] Lu Wei's speech at the China-ROK Internet Roundtable held on Dec. 10, 2013, http://cpc.people.com.cn/n/2013/1223/c64102-23923716.html.

sometimes abused and biased. The fourth way is the participation in different levels of institution building and promotion of cooperation in practical fields. This cooperation can be gradually expanded from an operational level such as cyber-crimes, and can even be started on case by case basis. At the same time, we should promote institution building in terms of cyberspace crisis management, cyberspace arms control and other cyberspace governance mechanisms.

2. The Forms of International Cybersecurity Cooperation and China's Actions

There are many forms of international cooperation in cybersecurity. In the past two years, China has shown strong cooperative willingness and been pushing forward international cooperation in cyberspace on bilateral, multilateral or international levels.

On the bilateral level, China has engaged in some forms of activities and cooperation with the United States, Russia, South Korea, UK and other countries. On July 8, 2013, China and America together set up the Sino-US Cybersecurity Working Group, under the framework of the strategic security dialogue, and held the first session of the network working group. In May 2014, five Chinese army men were prosecuted by the US Department of Justice, which led to China's decision to suspend the activities of the Sino-US cybersecurity working group. However, it still shows that China and the United States have created a mechanism of interaction. On Dec. 2, 2014, the Seventh Sino-US Internet Forum was held in Washington, DC. Mr. Lu Wei led a delegation to the session and delivered a keynote speech. In May of this year, China and Russia have just entered into a cybersecurity agreement, and reached a mutual understanding in the aspects of no cyber-attacks toward each other as well as joint research and development in technology. Actually, the Sino-Russian cooperation can be traced back to an earlier time. At the 66th United Nations General Assembly in 2011, China jointly drafted and submitted the initiatives for international cyberspace rules, which is "International Code of Conduct for Information Security", altogether with Russia, Tajikistan, Uzbekistan and other countries. The China-ROK Internet Roundtable Conference is held regularly between China and South Korea, with the second one held in Seoul, Korea on Dec. 10, 2013. Also, Britain and China have held an Internet Roundtable Conference. On Sep. 9, 2013, the Fifth China-UK Internet Roundtable was held in London.

On the multilateral and regional levels, BRICS, ASEAN, the Shanghai Cooperation Organization, Northeast Asia as well as the Asia-Pacific countries are all trying out a variety of mechanisms for cybersecurity cooperation. At the Fourth Senior Representatives session of BRICS National Security Affairs held on Dec. 6,

2013, in Cape Town, South Africa, it was decided to set up the BRICS Cybersecurity Working Group, and agreed to fight against cyber-crimes together. On the first China-ASEAN cyberspace forum held in Nanning, on Sept. 18, 2014, China reached the initiative to co-build a "China-ASEAN Information Port" along with Burma, Indonesia, Malaysia and other ASEAN countries, for the purpose of promoting multilateral development and cooperation in this region. The construction of the China-ASEAN Information Port encompasses five major platforms: infrastructure platform, technical cooperation platform, trade service platform, information sharing platform as well as a cultural exchange platform. In 2009, China and ASEAN also adopted the "Cooperation framework on the issue of cybersecurity for China-ASEAN Telecom Regulatory Council". The Regional Anti-Terrorism Structure Council of Shanghai Cooperation Organization's (RATS), at its 2013, March 22nd session in Uzbekistan's capital, Tashkent, reached agreement on urgent measures "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 Shanghai Cooperation Organization also entered into "Intergovernmental Cooperation Agreement between the member countries of Shanghai Cooperation Organization for the protection of international information security." From July 23 to July 24, 2014, the Ninth Asia-Pacific Information Security Conference (SecureAsia) was held in Beijing. From Sep. 24 to Sep. 25, 2014, the most authoritative annual summit in the field of Asia-Pacific information security, that is, 2014 China Internet Security Conference (ISC 2014), was held in Beijing. From Oct. 28 to Oct. 30, 2014, the 2014 Northeast Asia Peace and Cooperation Initiative Forum was held where the issue of cybersecurity cooperation in the region was one of its four major themes.

On the global level, China not only participates in various global and cross-regional cybersecurity sessions and activities, but also takes the initiative to build up a variety of international cooperation platforms. From Dec. 3 to Dec. 5, 2014, China actively took its part in the Fifth Global Cyberspace Cooperation Summit held in Berlin, which was jointly organized by the East West Institute from the US and the German Ministry of Foreign Affairs. 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 speech at the opening address themed as "A Cyberspace Shared and Governed by All" and put forward seven recommendations. As a member of the 15-member UN Group of Governmental Experts (GGE) - a body whose mandate is to study and build norms in the cyberspace - China agreed in a June 2013 report released by the GGE that UN 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 accord 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 cybersecurity. On June 5, 2014, China and the United Nations jointly organized the "United Nation International Symposium on Information and Cyberspace Security" in Beijing. From Nov. 17 to Nov. 18, 2014, Chinese Ministry of Foreign Affairs organized the Symposium on the Combat against Cyber Terrorism of "Global Counter-Terrorism Forum" in Beijing, around 70 representatives from nearly 20 member states and UN agencies altogether explored the theme of "Strengthen International Cooperation, Prevent and Combat Cyber-terrorism". From Nov. 19 to Nov. 21, 2014, the Central Network Security and Informatization Leading Group held the First World Internet Conference, attracting more than 1,000 participants from nearly 100 countries and regions around the world.

3. The Obstacles for Further International Cooperation in Cybersecurity

Surely, international cooperation in cybersecurity is of great significance, but we have to admit that it is still in a preliminary stage with more words than deeds in actual practice because its advancement is confronted with a number of obstacles. Firstly, from the perspective of perceptions, each country holds different views in terms of some basic cyberspace notions, such as Internet freedom and Internet sovereignty. Therefore, each country's demands in the course of international cooperation are also different. For example, the regulatory policies in cyberspace China implements are to balance security with freedom, in favor of the idea of internet sovereignty; meanwhile, the United States attaches great importance to unrestricted "Internet freedom", stressing the role of an open society in creating a 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 to break through China' restrictions on Internet access. In addition, each country also holds different standards in the issue of cybersecurity. The United States regards it as legal to carry out cyber espionage for security reasons, while such actions out of commercial reasons are considered illegal. However, most countries believe espionage activities for both reasons are unacceptable. In addition, the further expansion of international cooperation in cybersecurity is also affected by factors like different Internet penetration rates in different countries. For example, as for the countries with low Internet penetration rate, such as Mongolia and Brunei, their willingness to participate in international cooperation is quite low.

Secondly, from the perspective of institutions, a neutral dominant party is required for the further expansion of international cooperation and the coordination of international conflicts, however, there exist disputes about the role of a leading coordinator. For example, 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. With respect to the diversification of the governance body, emerging market economies and developing countries, such as China, make no objection. However, they do hope that international organization like ITU can create more initiatives, advocate the establishment of a fair and reasonable cyberspace governance mechanism, under the United Nations framework, that allows a broad participation of all countries.[34] The United Nations also believes that "the Internet has evolved into a global public facility. The 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".[35] Also, United Nations actively promotes the International Telecommunication Union to assume a leading role in Internet governance. However, these proposals from both the United Nations and China have been firmly opposed by the US government.

Finally, the biggest obstacle in terms of international cybersecurity cooperation stems from the inadequate strategic trust of each country on this issue. Based on the levels of trust, there are mainly three forms of strategic trusts, namely high level of trust, medium level of trust and low level of trust.[36] Among the relations in different countries, what the US and China have is regarded as low degree of trust. In different areas of Sino-US relations, in contrast with the fields of economy, politics and military, the Sino-US strategic mutual trust in cyberspace can be considered at the lowest level of mutual trust. As indicated by Kenneth Lieberthal, cyber is a realm in which the most hostile images each side has of the other are being reinforced. [37] Both

---

[34] Wang Xiaofeng, "The Cybersecurity Issues in Sino-US Relations," American Studies, No.3, 2013, p. 22.（汪晓风："中美关系中的网络安全问题"，《美国研究》，2013 年第 3 期，第 22 页。）.

[35] WSIS, "Building the Information Society : A Global Challenge in the New Millennium", Dec. 12, 2003, available at http://www.un-documents.net/wsis-dop.htm.

[36] J. B. Barney and M. H. Hanson, "Trust Worthiness as a Source of Competitive Advantage," Strategic Management Journal, Vol.15, 1994, pp. 175-190.

[37] Kenneth Lieberthal and Wang Jisi, Addressing U.S.-China Strategic Distrust, John L. Thornton China Center Monograph Series, Number 4, March 2012, p. 47.

countries hold significant doubts and worries about each other's actions and policies in cyberspace, which seriously affects both sides' strategic mutual trust with regards to cyberspace. Sino-US strategic mutual trust in cyberspace is one part of the overall Sino-US strategic perception. Therefore, inadequate strategic mutual or strategic distrust is decided by the status of the overall Sino-US strategic perception, which is affected by a variety of structural factors, including social systems, values, geopolitical factors, including the conflicts between great powers and rising powers. However, due to its unique nature, cyberspace has become a field where distrust in Sino-US strategic relations is most likely to be demonstrated and be amplified.

Conclusion

To sum up, China has its own unique cybersecurity perception, which is inseparable from China's national conditions. The cybersecurity in China's understanding must be interpreted under the framework of the Holistic National Security Outlook and the strategic goal of Cyberpower. China takes a more state-centric orientation toward cybersecurity. The cybersecurity interests in China's understanding are comprised of three aspects, that is, social and political stability, information infrastructure security, and cyberspace information and data security. And the corresponding major threats are "three forces" and other political cybersecurity threats, vulnerability from systems controlled by others as well as a variety of international cybersecurity games undermining China's security, economy and diplomacy.

After the Prism scandal, international cooperation in cybersecurity begins to enter the new era. The international community's consensus for the need to strengthen cooperation on cybersecurity began to rise. China has made efforts for cybersecurity cooperation on a number of international cooperation platforms, at the bilateral, multilateral, regional and global levels. China not only takes a positive role in various cybersecurity cooperation forums, but also actively builds up a variety of platforms for cybersecurity communication. In addition, China has already entered into a number of cybersecurity cooperation agreements or joint statements with associated countries. However, in order to further promote international cooperation in cybersecurity, there are still many obstacles to be confronted. For example, regarding perceptions, each country holds different understandings with respect Internet freedom and Internet sovereignty; at the institution level, each country holds different opinions with regard to cybersecurity governance as well as the institutional processes; and in the aspect of cybersecurity, strategic trust among countries is inadequate.

Indeed, cooperation in cybersecurity has become an international trend. For the common security of the global cyberspace, the countries must urgently strengthen their mutual trust in this area, recognize each other's internet sovereignty, reach a unified cyberspace code of conduct, clarify the common threats to cybersecurity, establish a sharing mechanism for network threat information, put hotlines in operation or enter into bilateral or multilateral agreements, and avoid possible misjudgment or occasional conflicts over issues such as cyber warfare at the expense of the security of the countries and the global network information system. As President Xi Jinping pointed out, the international community must be based on principles of mutual respect and mutual trust, through active and effective international cooperation, work together to build a peaceful, secure, open and cooperative cyberspace, and establish a multilateral, democratic and transparent international Internet governance system.[38]

[38] President Xi Jinping's message of congratulation in the First World Internet Conference, Nov. 19, 2014, http://news.xinhuanet.com/live/2014-11/19/c_127228771.htm.