The Way Ahead: Cyber Relations between China and the US*

Zhu Qichao †

Since 2010, cyber security has become one of the important issues that are of great impact on the relationship between China and the United States, along with the increase of China's comprehensive national strength and expansion of its national interests in cyberspace. Many cyber security topics, such as cyber freedom, cyber sovereignty, hacker attack, intellectual property theft, code of conduct in cyberspace, have frequently been mentioned by think-tank scholars and government officials of both China and the US, with each blaming the other side. From June 5, 2013 when the former National Security Agency (NSA) employee Edward Snowden disclosed the scandal of PRISM on the British newspaper *The Guardian* to May 19, 2014 when the US Department of Justice prosecuted five Chinese military officers for "cyber espionage," the fierce verbal confrontation on cyber security issues between China and the US had caught international concern. As Kenneth Lieberthal and Peter W. Singer said in the Brookings report "Cyber Security and US-China Relations," "There is perhaps no relationship as significant to the future of world politics as that

* This article is originally written in Chinese.

† Director and associate professor of the Center for National Security and Strategic Studies (CNSSS) , National University of Defense Technology, China. The author is grateful for the anonymous revising advice from the experts of Institute for International and Strategic Studies, Peking University, and also grateful for the manuscript translation help from his two colleagues, Dr. Zhao Zhao and Ms. Wendy Wang.

between the US and China… In the web of relationships that have built up between the US and China, no issue has emerged of such importance, and generated such friction in so short a time span, as cyber security."[1] In spite of the frictions, limited communication and cooperation on cyber security issues has also been carried ourt between the two nations, which has helped ease the tensions and facilitates strategic trust between the two countries. Generally speaking, the China-US game over cyber security has turned into a more and more influential factor that will produce a profound and lasting impact on the bilateral relationship in the future. Proceeding from the perspective of China-US interactions in the domain of cyber security, this paper analyzes the short history and major problems in China-US cyber security cooperation, and then makes some suggestions on how to promote the new model of relationship between major countries and offers certain policy recommendations for Chinese governmental institutions.

1. Major Differences on Cyber Security between China and the US

Significant differences between China and the US in such aspects as political system, ideology, stages of development, history and cultural traditions, it is thus inevitable for the two countries to have different views on cyber security-related issues, on four aspects in particular, i.e., cyber freedom and cyber sovereignty, cyber-hacking, international Internet governance rights, and cyber arms control and the international code of action in cyberspace.

1.1 Cyber Freedom and Cyber Sovereignty

With the rapid development of Internet and new media technologies, people around the world are realizing that internet-related social media tools, such as Facebook and Twitter, have a growing impact on national security and social stability. Both the speeches on Internet freedom made by former US Secretary of State Hillary Clinton in 2010 and 2011 and the US government report entitled "International Strategy for Cyberspace" published in 2011 expressed clearly what the US has been really advocating

on the issues of cyber freedom and cyber sovereignty. From the viewpoints of the US government, on one hand, the basic freedom in cyberspace should be protected, and the freedom of being interconnected and information communication should not be restricted, and major countries such as China and Russia should not conduct any Internet content filtering or censorship. On the other, however, the US always has a tendency to take advantage of the so-called cyber diplomacy and cyber smart power to intervene or even overturn the governments of its enemies, which has been witnessed on more than one occasions, such as in the Iranian presidential election, the Google Crisis, and the "Jasmine Revolutions" in the Arab world. From the Chinese government's point of the view, there is no such a thing called "absolute cyber freedom," and every country should comply with the UN Charter and the universally accepted basic norms governing international relations, including respecting a country's sovereignty, territorial integrity and political independence; respecting human rights and fundamental freedoms; and respecting the diversity of history, culture and social system of all countries. In cyberspace, the principle of combining sovereignty with free and safe flow of information should be observed to prevent the cyberspace from becoming a new tool to interfere in others' internal affairs; in particular, cyber freedom should never be employed as a tool for cyber supremacy.[2] According to the Rand report entitled "Internet Freedom and Political Space" released in September, 2013, the Bureau of Democracy, Human Rights and Labor of the US State Department once commissioned the Rand Corporation to start a monographic study on "the impact evaluation of Internet freedom on elective governments" one year after the Google Crisis. The objects of the study include Egypt, Syria, Russia and China, and the contents of the study covered such subjects as what impact Internet freedom of speech could have on the realistic political situation, and which countries would be influenced more outstandingly by Internet freedom than others, and how should be done to maximize the effectiveness of the Internet Freedom Initiative pushed by the US government, and so on.[3] In the view of Chinese government and scholars, those criticisms on China made by Hillary Clinton and this report serve

as specific evidence of the US government's interference in other countries' internal affairs in the name of cyber freedom.

1.2 Cyber Hacking

In recent years, as a new type of threat to international order, hacking has become more and more rampant, since in cyberspace offense is easier than defense. According to a CSIS report entitled "The Economic Impact of Cybercrime and Cyber Espionage" released in 2013, the US alone lost almost US$160 billion annually due to cybercrime, which accounted for about 1% of its annual GDP.[4] China's Internet security situation is not optimistic, either. According to the CNCERT report, "China's Internet and Network Security 2012," released in July, 2013, the theft of financial information had become one of the major goals of hackers. In China, the personal information of more than 50 million internet users were sold illegally, the number of domestic websites deliberately falsified reached 16,388, and 52,324 websites were secretly implanted with some backdoor malwares in 2012 alone.[5] At the 4th Global Cyberspace Co-operation Summit held on November 5, 2013, Mr. Cai Mingzhao, the then director of Information Office of the State Council, pointed out that more than 80% of Chinese internet users experienced some kind of cyber threat and attack or another, causing a total economic loss and damage worth dozen billion US dollars. Some western countries, especially the US government, think tanks and news media, have always tended to slander others when they suffer cyber attacks, accusing China, Russia or other countries of stealing their technological and commercial secrets. The so-called APT1 report made up by the American cyber-security firm Madiant Co. even lodged up a false cyber charge against the Chinese military. In 2013, the former US NSA employee, Edward Snowden, gradually disclosed a massive Internet surveillance program named PRISM, the sniffer on those state leaders of Germany, France, and China, and the hacking penetration behaviors against the organizations abroad carried out by the NSA. Although the US government persisted in saying that the disclosed cyberspace monitoring behaviors were performed for national security, and the collected

information were not transferred to any of the US companies for commercial purposes, the so-called "PRISM Gate" still strongly undermine the Americans' arrogance of always blaming others on cyber security issues.

On March 24, 2014, while attending the Hague Nuclear Security Summit in Netherland, Chinese President Xi Jinping criticized the NSA for invading Huawei Co.'s servers and for monitoring former Chinese leaders when meeting with the US President Barak Obama. President Obama argued that the American surveillance programs were for the good of national security instead of commercial interests. On May 19, 2014, the US Justice Secretary Holder hosted a news press conference with some FBI officials and declared to indict five Chinese military officers for "cyber espionage," which invited again strong reactions from the Chinese government and the general public opinion on the fact that the US is playing a trick of a thief crying "stop stealing". On the other hand, US government officials, members of Congress and even the US public opinion tend to believe that the so-called American national-security-oriented cyber spying is nobler than the so-called Chinese economic-interests-oriented cyber spying.[6] Such a weak self-defense certainly was not persuasive to the Chinese government and the Chinese people at all, which further eroded the original fragile trust between the two sides. The report "The Global Monitoring Action Record of the US" was released by the Chinese Internet News Research Center under the State Council Information Office, PRC one week after the US declaration of the prosecution against the five PLA officers. It outlines the US global massive monitoring actions in the name of protecting its national security. We can see that the Chinese government and official news media keeps high vigilance towards the US's selfish motive, which is to seek global hegemony with its supremacy of information technology in cyberspace.[7]

The US and China are holding different positions on the issue of combating cyber-crimes too. After joining "The Budapest Cybercrime Convention," the US requested any country to sign the convention to combat cybercrimes jointly. China always firmly opposes any kind of cyber hacking behavior, but because of some inconsistencies between specific Convention's terms with

the Chinese domestic realities, China has not signed it yet. China, Russia and some other countries want to coordinate their respective positions within the frame of the UN, and appeal to strengthen international cooperation to prevent the illegal abuse of information technology.

1.3 International Internet Governance

Cyberspace is generally accepted as a global public domain, which has played an important role in promoting international information communication, technological innovation and economic globalization. However, due to growing dependence on the Internet worldwide, cyber security has gradually grown into a global challenge, and more and more attention has been given to the topic of international internet governance rights all over the world. As the birthplace of the Internet and an IT superpower, the US monopolizes the management of Internet operation and related strategic resources. At present, among the total 13 Internet root severs of the planet, the only primary one and nine supplementary ones are located in America. And the Internet Corporation for Assigned Names and Numbers (ICANN) under the control of the National Telecommunication and Information Administrative of the US Department of Commerce for a long time is the unified administrator to all of these root servers, which provides DNS and IP addresses management services to the global Internet users. Before the 1990s, the contradictions in relation to the Internet governance was not yet much prominent for low dependence of various countries on the Internet. Since the early 21st Century, the US continuous practice of taking advantage of its monopolized control over the Internet to achieve political and strategic objectives have aroused the wariness of the international community. For example, during the 2003 Iraqi War and the 2004 Libya-US dispute over the issue of top-level domain name management, the US terminated the DNS services for the Iraqi and Libyan top-level domain names ".iq" and ".ly," and made these two counties' websites disappear from the Internet for several days. In 2009, Microsoft also temporarily shut down the MSN services for such countries as Cuba, North Korea and Sudan. With each country's

growing political, economic and social dependence on the Internet, China, Russia and some EU member countries have come to be aware of the critical relations of Internet domain governance with national sovereignty and security, and proposed to establish in the United Nations an international institution similar to the International Telecommunication Unions to replace the ICANN to manage and allocate Internet domain names and IP addresses.[8] On March 14, 2104, the National Telecommunication and Information Administration under the US Department of Commerce declared that the US government was willing to hand over the critical Internet domain names' administrative functions to an organization of global stakeholders, but under the pre-condition that as the first step of handing over the Internet governance rights, all the stakeholders should be called together to form a transfer program with "broad international support". Such a declaration could be considered as a compromised response to the world opinion pressure caused by the Edward Snowden exposure, but still be far away from shifting Internet governance out of the American shade. Technically speaking, partially handing over the administration of the Internet domain names from the ICANN is just a limited measure to keep the Internet open, and it should not be interpreted or understood that the US really wants to give up the control of the Internet.[9] According to the PRISM project and the future key investment programs, the US government will try its best to maintain a global leadership in the area of information technology, and to maintain American superiority in controlling and utilizing the Internet. Judging from the trends of reform of international Internet governance, the US government will continue to slowdown this process with such excuses as "national security" and "difficulty in reaching a broad international support." Since 2010, the number of the Chinese Internet users, especially the mobile Internet users, has been growing rapidly. China's national interest has become increasingly dependent on cyberspace, and China has become an important Internet stakeholder. It's an inevitable topic for both China and the US to discuss how China can have a greater voice, influence and responsibility in the reform of international Internet governance.

1.4 Cyber Arms Control and International Code of Action

IT and network technologies have promoted the development of economic globalization and social informationization. They have also made critical infrastructure systems, such as financial and securities information systems, power grids, transportation management information systems and massive industrial control systems, among others, more and more dependent on cyberspace, in addition to making military affairs more and more cyber-dependent. In its 2010 new version of military strategy, the US defined cyberspace as a new independent operational domain. In order to keep up with the development of the world's new military revolution, almost all major military powers have released their own cyber security strategies, established cyber war forces, and the arms race in cyberspace is heating up. At the beginning of 2013, to ensure an absolute superiority and freedom of action in cyberspace, the US Department of Defense decided to strengthen its Cyber Command by greatly increasing the number of personnel working in it from 900 then to 4,900 in 2015. On March 30, 2014, the US Defense Secretary Hagel said again that the staff in the Command would be further expanded to 6,000 by the end of 2016. At the same time, the US military has developed more than 2,000 kinds of cyber malware weapons, such as "Stuxnet" and "Flame," and conducted a series of cyber exercises, such as "Cyber Strom" and "Schriever." To support its move of cyber arms expansion, *The Tallinn Manual*, i.e., *The Manual on the International Law Applicable to Cyber Warfare*, organized and co-authored by Prof. Michael N. Schmitt of the US Naval War College, was released on the NATO official website in March 2013. The major points in this manual include: national sovereignty and governance of cyberspace should be recognized; cyber attack beyond a certain size or caused a certain impact is a type of "armed attack"; cyber attack behavior conducted by individuals or organizations is equal to that conducted by a nation; conventional armed forces could be used to counterstrike a cyber attack; the principle of collective self-defense among allies is applicable to cyberspace; cyber attack against important civil targets, such as hospitals and children welfare institutions, should be prohibited; and the Neutrality Law is applicable in cyberspace,

etc.[10] The release of *The Tallinn Manual* indicates that the US and NATO wish to dominate the making of international code of cyberspace conduct, and set a legal basis for starting a war in cyberspace. Given that the US has already established some powerful cyber war capabilities, the acts of setting cyber war rules and legitimizing cyber war would definitely intensify the doubts from the BRICS and other developing countries. As early as 2011, four members of the Shanghai Cooperation Organization — China, Russia, Tajikistan and Uzbekistan — submitted a written proposal entitled "The International Information Security Code of Conduct" to the United Nations. Unfortunately, the proposal did not gain sufficient attention and positive response from the Western countries, especially the US.

The US and NATO wish to dominate the making of international code of cyberspace conduct, and set a legal basis for starting a war in cyberspace.

2. China-US Dialogues on Cyber Security

In order to reduce friction and confrontation and keep China-US relations on the right track, the two countries have conducted multiple types of cyber security dialogues and cooperation since 2009, which can be divided into two levels: non-governmental and official.

2.1 Cyber security Dialogues at Nongovernmental Level

The officially authorized Track II talks and the conferences held by the academic institutions on the two sides are the two major forms of non-governmental communication between China and the US on the cyber security issues. The cyber security conferences turn primary attention to academic exchange, the topics of discussion are relative flexible and cover such hot issues as the definition of basic terms in cyber security studies, the impact of cyber security on international relations, different attitudes of China and the US towards the hacking problem, and the prospect for future China-US cyber security cooperation. Take the International Seminar on the Strategy

of National Security and Development of Science & Technology sponsored by the National University of Defense Technology since 2009 for example. Experts from US universities and think tanks were invited each time to participate and they joined their Chinese counterparts in discussing many issues, such as cyber security and cross-domain security. The seminars gave the attendees extensive room of discussion that not only facilitated mutual understanding but also played the role of academic diplomacy to some extent.[11]

Since 2009, at least three Track II communication mechanisms have been established between China and the US. The first one is the China-US Cybersecurity Dialogue launched jointly by China Institute of Contemporary International Relations (CICIR) and the Center for Strategic and International Study (CSIS), which has been held for eight rounds. Scholars and government officials in the capacity of observers from both sides have held continuous discussions about such issues as China-US cyberspace mutual trust mechanism, formulation of international code in cyberspace, China-US cooperation on combating cyber crimes, and response to new security challenges in cyberspace. The second one is the cyber security dialogues and seminars organized by the Brookings Institution. The major achievements of these activities are expressed in *Cybersecurity and US-China Relations* authored by Kenneth Lieberthal and Peter W. Singer, and *Addressing US-China Strategic Distrust* written by Wang Jisi and Kenneth Lieberthal.[12] The third one is the periodic dialogues sponsored rotationally by the China Foundation for International Strategic Studies (CFISS) and the CSIS Pacific Forum, which set more and more cyber security-related topics on the agenda in the recent years. These bilateral dialogues gave decision-makers on both sides a lot of positive and constructive messages, and facilitated the understanding of each other's goals and concerns, promoting the establishment of norms of cyber conduct and thus helping lay a foundation for mutual trust and cooperation between China and US.

2.2 Cyber Security Dialogues at the Official Level

With the rising importance of cyber security issues in China-US relations, governments of both countries have attached great

importance to them and conducted more and more cooperation through three channels. The first channel is high-level dialogues between the governments. Besides discussions about cyber security issues in meetings of the heads of states, the issues also gained much attention during the China-US Strategic Security Dialogue since 2011 under the framework of the China-US Economic and Strategic Dialogue that was established in 2009. The second channel is the communication and cooperative mechanism between the two countries' functional departments. At present, China and the US are conducting effective cooperation by means of the Joint Law Enforcement Contact Group on such issues as combating cybercrimes, intellectual property law enforcement and justice assistance, among others. For example, in August 2011 the police of China and the US jointly cracked down on Sunshine Entertainment Alliance, the biggest Chinese-language pornography website in the world. In April 2013, the governments of the two countries decided to establish a Cyber Issue Working Team to coordinate the two sides' positions and accommodate differences. On July 8, 2013, the first meeting of the Team was held under the framework of strategic security dialogue by both governments. Issues such as mechanism construction, cyber relations between the two countries, international norms of cyberspace and means of bilateral dialogue were discussed frankly. However, on May 19, 2014, only one year after the establishment of this group, the US Department of Justice prosecuted five Chinese military officers for so-called cyber espionage. The Chinese government held that the US actions seriously violated basic principles of international relations, damaging the cooperation and the mutual trust between two sides. Furthermore, the US lacked the sincerity to solve problems through communication and cooperation. As a result, the Chinese government decided to suspend relevant activities of this China-US Cyber Issue Working Team, and started a cyber security background scrutiny mechanism targeting foreign IT enterprises. The third channel is the cooperation between experts from both sides under the framework of the United Nations. In June 2013, experts from China and the US participated in a multilateral UN discussion on subjects of cyber security, which reached some limited

agreement on acknowledging the concept of cyber sovereignty, but more disagreement remained on the connotation of the so-called cyber sovereignty and the code of action in cyberspace.

2.3 Limitation of China-US Cyber Security Dialogue and Cooperation

Judging by current situation, the China-US cyber security dialogue displays three characteristics. The first one is that the US holds an obvious offensive posture, and China is in the defensive. The US is usually the side that drops topics in such areas as cyber freedom, cyber hacking, IP protection and code of conduct in cyberspace, attempting to seize and keep the commanding height in moral terms, while China is always the one side forced to take up the challenge passively and hold fast to a bottom line. The second one is that there have been much discussion about the definition of specific terms but less about substantive issues. Despite the numerous rounds of academic exchanges between academic circles of the two countries, much incongruence still remains in the understanding of some basic cyberspace-related terms. Moreover, due to the gap of development in the two countries' social informatization, much difference exists in the understanding of the cyber security issues between the two sides. Third, there has much discussion by which the two sides wish to understand the other side's bottom line. It is particularly so for the US side which in recent years has put the issues of cyber security, space security and nuclear security in the same breath, indicating the foundation of mutual trust between the two sides in high-tech areas remains quite fragile. On the part of the US, it tends to believe that the development of China's space and cyberspace technologies has reached a stage to pose a real threat to it. On the part of China, however, it holds that the US enjoys great technological advantages in cyberspace, outer space and nuclear power, and thus harbors great worries about its own security in these areas.

As Friedrich Engels once said in *Conditions and Prospects of a War of the Holy Alliance against France in 1852*, humans fight in the way they produce.[13] For nation states, especially the big powers, when their national interests are expanding inevitably

into cyberspace, they have to consider defending their security and development in cyberspace as their most important national interests, and pursue the development of their own cyber military capabilities and build their own cyber national defense forces. Since the early 1990s, as a leading advanced country in all cyber-related areas, the US has been improving its national cyberspace security strategy. It now has formulated a strategic system that includes an international cyberspace strategy, a national cyberspace strategy and a military operational cyberspace strategy. The national interests in cyberspace are regarded a cornerstone of its national security and economic prosperity.[14] For China as a big developing country rising rapidly, its strategic readiness to meet challenges to its cyberspace security lags behind the growing dependency of its national interests on cyberspace. On November 13, 2013, the resolution of the Third Plenary Session of 18th Central Committee of Communist Party of China (CPC) announced the establishment of the National Security Commission of CPC, and on February 27, 2014 the Central Leading Group of Cybersecurity and Informationization was established, indicating that the Chinese government has eventually elevated cyber security to the level of national security. From the perspective of national security decision-making, China's strategic readiness in terms of cyber security falls about 10 or even 20 years behind that of the US. Moreover, in China -US relations cyber security issues are often mingled with geopolitical issues, maritime disputes, economic and trade problems and intellectual property disputes, thus greatly increasing the difficulty for the two sides to establish mutual trust in cyber security. In the fields of outer space and cyberspace, where a lot of blank areas still exist in technological and governance capability, it is even harder to dispel misunderstandings between the two sides than in the traditional fields. Therefore, the cyberspace will become a main field of competition between China and the US in terms of security, military affairs, intelligence,

The cyberspace will become a main field of competition between China and the US in terms of security, military affairs, intelligence, technology and even ideology.

technology and even ideology.[15] Since cyber security has permeated into economy and trade, politics and diplomacy, military and national defense in the China-US relationship, it has become so important that it highlights the confrontation-side of the bilateral ties. The increasing significance of cyber security in this relationship may challenge the foundation of China-US cooperation established after the September 11 Attacks, and cast some negative impact on the development of a new-type major power relationship between China and the US.[16] For the limitations mentioned above, the China-US cyber security cooperation is still at the primary stage.

3. Obstacles in China-US Cooperation on Cyber Security

With the further extension of the national interests of both China and the United States into cyberspace, the demand for cyber security cooperation will become increasingly stronger between the two countries. Benign cooperation in this regard will definitely facilitate the development of the new-type bilateral relationship between the two major countries. But, it must also see that there are also some obstacles affecting cyber security cooperation between China and the Unites States. Apart from the long-standing structural problems in the fields of economy and trade (such as the problems of trade deficit and RMB exchange rate) and the Taiwan issue and so on, primary attention need to be paid to the following three immediate issues.

3.1 How the United States would handle the negative impacts on China-US strategic relationship caused by its "Asia-Pacific rebalancing" strategy.

Since 2009, the United States has "pivoted" to Asia in a high profile and implemented the strategy of "Asia Pacific Rebalancing". The strategy mainly includes the Trans-Pacific Partnership Agreement (TPP) in the field of the economy, the Air-Sea Battle Concept with China as the imaginary enemy and other related contents. On the specific terms of military deployment, the United States recently decided to deploy 60% of its global military force to in Asia-Pacific region, and deploy a number of advanced weaponry,

such as the Global Hawk UAVs, the F-22 stealth fighters and F-35 fighters to the periphery of China. In terms of operational scenarios, the United States considers the future cyber warfare as a significant part of its Air-Sea Battle Concept.[17] These initiatives will inevitably increase pressure on China's national security and make China more worried about its security, and consequently cast a lingering shadow on future China-US cooperation on cyber security.

3.2 Whether the United States would willingly accept China's advocacy of the "new-type relationship between major countries".

In recent years, Chinese leaders put forward the concept of "new-type relationship between major countries," the connotation of which is "no conflict, no confrontation, mutual respect, cooperation and win-win". This is a new concept China proposes on the basis of the universally accepted norms in international relations, giving expression to China's sense of responsibility and style of doing things as a large developing country. But, the United States is a country that believes in the principle of power, and maintaining American global hegemony is the basis of its national security strategy. It is not optimistic whether the United States is willing to accept China as an equal partner rather than a potential strategic rival. From April 23, 2014 to April 29, the US President Barack Obama visited four Asian countries, supporting its military allies to confront China. Judging by this, it is unlikely that the United States abandons the mentality of Cold War and the policy of containment against China. Dr. Kissinger once used the term "Crowe school of thought" to refer to a group of American intellectual elite who firmly believe that China's rise will conflict with the national interests of the United States. Currently, the views of these elite have a considerable market in the US political, business and academic circles. Before World War I, Eyre Crowe, then a British diplomat, wrote to the British Foreign Office a confidential report on the rise of Germany, known as the "Crowe Memorandum". It argued that no matter how the "Rising Country" behaves, its rapid development of power would lead to the incompatibility between itself and the survival and development

of the existing hegemonic country. The "Crowe school of thought" derives from this report.[18] Thus, China and the United States may have different understandings of the "new-type major country relationship," which may, in turn, affect the development of bilateral strategic mutual trust, as well as China -US exchanges and cooperation in relation to cyber security issues.

3.3 Whether the United States will practice self-restraint in the development of its cyber arms.

The United States is a country with the world's most powerful military strength; it is also a nation boasting the largest scale of and the most powerful cyber arms. The high-profile military buildup of the US Cyber Command since 2013 has become the justification for other countries' development of their own cyber force. For China, the United States, Russia and other major countries, arms race in cyberspace will exacerbate the strategic mutual distrust among them. US scholars David C. Gompert and Philip C. Sanders recently proposed the concept of "strategic restraint," calling on Russia, as well as the United States and China to strategically restrain one another in the nuclear, space and cyberspace fields. But, other countries will have a stronger sense of insecurity if the United States, the country boasting the most powerful force, cannot enforce self-restraint.[19] In recent years, some US experts have also come to conclude that it is the United States rather than China that is pushing the arms race in Asia.[20] This indicates that, if the United States does not adjust its Asia-Pacific security strategy and policy, what follows will be an endless arms race in the region, which will erode continuously the fragile China-US strategic mutual trust.

3.4 There exist cognitive differences on cyber security issues between China and the US.

It is likely that cyber security issues affect China -US exchanges in various fields. Yet, differences in the level of social informationization, legal system and political system between the two countries not only make their dialogues superficial but also give rise q number of cognitive dislocations. The first cognitive dislocation is related to the IT edge. China is the biggest developing

country with a great potential; it has long held that the United States has unrivalled advantages in high technology throughout the world, particularly in Information and Communications Technology (ICT). The "Big Eight" of American ICT giants, including Cisco, Google, Oracle and Microsoft, among others, are often regarded to have a technological monopoly. In the ICT domain, China is considered still much inferior to the US, and naturally many people are even worried that China's cyber security system may not perform effective functions when dealing with the powerful American technological advantages. On the part of the United States, however, it holds that, due to the fast proliferation of technology and low threshold of innovation, the big Chinese IT companies, such as Huawei and ZTE, have been growing faster and faster, and they may even achieve a comparative advantage in certain specific areas over US companies. Therefore, the United States is concerned that its cyber security may no longer be as absolutely reliable as usual. The second cognitive dislocation is about hackers and cyber espionage. Based on the disclosure made by Edward Snowden, China has come to realize that the American capabilities in signal monitoring and its network surveillance technology are beyond comparison, and the intelligence collection by the US has covered all aspects, politics, economy, military, and science and technology included, indicating that the US has been doing all possible to maintain its advantages in all these areas. In view of such facts, the United States admits that it does indeed performs large-scale Internet surveillance, but argues that it is mainly done for the purpose of national security. Members of Congress and some retired senior officials are worried that China may use cyber espionage to obtain American commercial secrets and encroach upon American intellectual property rights. They worry that, if China continues to develop its cyber capability, there will be huge losses in American national wealth in the long run, and the US's edge in high technology upon which its hegemony depends would be in jeopardy.[21] The third cognitive dislocation is on cyber security legislation and law enforcement. Since the Snowden incident, public opinion in China has been focusing mainly on the moral hypocrisy of the United States. Yet, the government, high-tech firms,

universities and research institutions in the United States have been focusing on employing legal means to restrain the so-called Chinese hackers and related cybercrimes. Some American think tanks stirred up controversies. For example, the Mandiant Co. elaborately cooked up "evidence" to frame five Chinese military officers and then the Department of Justice indicted them. All these actions suggest that the United States is trying to dissociate its network espionage from cybercrime and press China through its skillful legislation and law enforcement. These cognitive dislocations on cyber security between China and the United States will continue to profoundly influence cyber security strategies and related policies of the two countries. They may be foreshadowing cyber security conflict, and hinder further dialogue and cooperation between the countries.

4. Policy Suggestions on Promoting Pragmatic Cyber Security Cooperation between China and the US

China suspended the Sino-American Cyber Security Working Team dialogue because of the US Department of Justice's prosecution of five PLA officers. However, along with closer interdependent links, "bucket and not broken" has become an unstated agreement in the bilateral relations between China and the US. The United States is likely to take the initiative to ease cyber security tensions and continue to maintain communication and dialogue during the new round of Strategic and Economic Dialogue to be held. In general, Sino-American cooperation in cyber security has not only constraints but also opportunities. Looking into the future, if the United States can really treat China as an equal partner and accept the construction of a new-type major country relations advanced by China, a foundation of mutual trust will be established and consolidated through pragmatic cooperation, and the barriers affecting cyber security cooperation between the two countries will be removed. It should be pointed out that the China-US competition in the field of cyber is based on their competition of national strength, and that their cooperation is also anchored in their national strength. If a great disparity exists between the two

major countries in strategic decision-making capacity, IT capability and cyber defense strength, it is impossible to have true equal bilateral cooperation in dealing with cyber security challenges. The process of building up strength in cyber security by any sovereign state is also a course of pursuing its cyber power. Cyber security is closely related to all aspects of relations among major countries. In essence, the cyber power can be divided into three components: the procedure power based on the code of conduct in cyberspace, the resource power to influence cyberspace, and the structural power based on the control of cyber information infrastructure.[22] For China, it should facilitate Sino-American cooperation and dialogue while making efforts to strengthen the foundation for bilateral cyber security dialogues. It is important for China to strengthen its cyber security capability, make good use of its cyber resources, and further enhance its strategic initiative in future Sino-American cyber security relations. China should take actions in the following areas:

4.1 To strengthen power of discourse on cyber security issues

As shown above, China has a quite weak voice and its ability to lead the discussion on related issues is now strong in joint Sino-American seminars or workshops on cyber security. This reflects, on the one hand, the reality that the two countries have cognitive differences concerning cyber security issues because of their different levels of informationization, and on the other, the need that China's research in cyber security remains to be deepened and that its transmission mechanism of cyber security policy is not yet well established. For example, China issued as early as June 2008 The Outline of National Intellectual Property Protection Strategy in order to protect intellectual property rights and crack down on intellectual property infringements by way of improving relevant institutions as well as legislations. Yet, China remains weak in responses to accusations made by the US side on IP theft in recent years, indicating that China is not yet good at publicizing and explaining to the international community its cyber security-related policies. Therefore, it is necessary for China to pool research resources of the government, enterprises and academic institutions to carry on continuous research in such areas as cyber

security-related concepts (terminology), cyber security strategy, relevant laws and regulations, industrial policies and infrastructure; to establish "a grand view of talents," break the cognitive bias of "it is a matter for the technicians whenever cyber security issues arise," adopt a variety of flexible measures to train talents in various relevant fields, such as cyber diplomacy, cyber governance, cyber technology, cyber legislation, cyber security industry policy, and cyber infrastructure, etc., so as to make research in cyber security more professional and uplift it a higher level; to use white papers, the bilateral dialogue mechanism, academic exchanges between the think tanks of the two countries and other means to show China's cyber security strategy and policies as well as its sincerity for cooperation on cyber security; and to enhance the legislation and law enforcement effectively in this regard; to set up a special cyber security crime investigation agency, pool governmental resources and social capital to develop a new generation of traceability technology, so as to establish an evidence chain directed against all kinds of cyber crimes aimed at China from the US territory, so on.

PRISM has greatly damaged the image and moral credibility of the United States in the eyes of the global public, and showed that Uncle Sam's hacking espionage to its citizens and targets of other countries is far beyond people's imagination, and the US is misusing information technology to pursue and consolidate its hegemony.

4.2 To jointly promote formulation of international code of conduct for information security

Edward Snowden's disclosure of the mass surveillance plan of National Security Agency still casts a long, dark and inescapable shadow over the cyberspace. The mass surveillance caused the international community, including important alliances of the United States, a wide outcry. PRISM has greatly damaged the image and moral credibility of the United States in the eyes of the global public, and showed that Uncle Sam's hacking espionage to its citizens and targets

of other countries is far beyond people's imagination, and the US is misusing information technology to pursue and consolidate its hegemony. The disclosure, however, provides the international community a good opportunity to reform and improve international cyber security governance. As such, China should meet the wishes of the general public in cyberspace, and work to unite the vast members of the international community, including developing countries and the United States, to promote the formulation of an international code of conduct for cyber security under the UN framework. The code of conduct must be based on a wide range of consensus and enjoy public confidence, so the scenario of an unlimited arms race in cyber space may be avoided. In fact, as its national interests become more and more dependent on cyberspace, it is inevitable that China becomes a more important stakeholder in global public domain of cyber security, and therefore take more responsibilities on issues concerning international cooperation in cyber security, and fulfill corresponding international obligations in more active ways.

4.3 To urge the United States to open its market to Chinese IT enterprises

In recent years, the United States has frequently been using national security as an excuse to block Chinese high-tech IT enterprises, like Huawei Co. and ZTE, to enter the American market. At the same time, American high-tech companies, such as Cisco, IBM, Google, Qualcomm, Intel, Oracle, Microsoft, Apple and others, have taken up a lion's share of the information infrastructure market in China's telecommunication, finance, energy, transportation and other key economic sectors. This seriously asymmetric phenomenon is the result of the interference of the US Congress on the competition of the international IT market, and it also shows the unequal and unfair treatment the United States gives to Chinese IT products. Various countries will naturally increase interdependence with more and more use of the Internet. The interdependence between the United States and China, however, is established upon asymmetric information infrastructure resources, which constitute major mutual prevention, resulting in the security

dilemma for both sides, especially for China. If no measures are taken to ease this situation, the distrust of the Chinese government and Chinese business community for the United States on cyber security issues will exacerbate. For China, it needs to enhance mutual trust and cooperation on cyber security issues with the US; yet, it is also necessary for it to strengthen its security system in scrutiny of the foreign high-tech products supply chain and take practical steps to push the United States to equally open its IT market for Chinese enterprises as soon as possible. Otherwise, the security concerns on IT product penetration and related trade disputes will sour bilateral mutual trust and cooperation.

4.4 To continue multi-level bilateral dialogue and cooperation

China and the United States have cooperated fruitfully in fighting against cybercrime. In the future, they will continue to deepen cooperation in obtaining technical evidence and law enforcement. This would help China improve the building of its relevant legal system and strengthen its law enforcement capability to cooperate better with the international community in cracking down on cyber hacking and foster its image as a responsible major country. Up to now, China and the United States have established approximately 100 consultation and dialogue mechanisms at different levels in the political, economic and military fields, which serve as valuable institutional resources for both countries to reduce direct conflicts and promote cooperation.

The usual pattern for the formation of these consultation and dialogue mechanisms are: first tested as the level of Track II between non-governmental organizations and think tanks before being upgraded to the level of Track I dominated by government functional departments when the communication becomes mature. Usually, when the dialogues are upgraded to the level of Track I, those at the level of Track II would stop. Therefore, it is necessary to keep and explore dialogues and cooperation at multiple levels to create a situation of dialogue at multiple tracks and levels, so as to ensure sufficient and sustained communication and understanding between the two countries before dialogue and cooperation start at the level of Track I.

Apart from tackling cyber relations with the United States, China has been actively engaged in bilateral or multilateral dialogues in relation to cyber security with the United Kingdom, ASEAN, the European Union and Africa Union; it is trying to carry on even more substantial cooperation with all relevant parties. Actually, China has been conducting cyber dialogue and cooperation with the members of Shanghai Cooperation Organization and the Republic of Korea early. The Wuzhen World Internet Conference, which closed on November 21, 2014, serves as a milestone event for China to sponsor and organize the first international convention on cyber issues to make China's voice heard. President Xi's letter of congratulations to the conference clearly expressed China's vision on cyberspace. It states that, following the principle of mutual respect and mutual trust, China is ready to work with all other countries to deepen international cooperation, respect sovereignty on the Internet, uphold cyber security, and jointly build a cyberspace of peace, security, openness and cooperation, as well as an International Internet governance system of multilateralism, democracy and transparency. Boasting 632 million Internet users, China has been a lucrative market for all Internet giants, which means a lot for the future of China-US cyber relations.

---

1 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The 21st Century Defense Initiative at Brookings and the John L. Thornton China Center at Brookings report, February 23, 2012, p.1.

2 Yi Wenli, " China-US Differences in Cyberspace and Their Cooperation Path" (in Chinese), carried in *Contemporary International Relations* (Monthly), Beijing, July 2012 Issue 7, pp.28-33.

3 Oleseya Tkacheva, Martin C. Libicki, et al., *Internet Freedom and Political Space*, RAND Corporation report, September 2013, p. iii.

4 CSIS and McAfee Report, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013, p.5.

5 "Domestic Information Security Hot Spots," *China Information Security* (in Chinese), August 2013, p. 14.

6 Shane Harris, "Our Spying Is Better Than Your Spying," May 31, 2014, available at: http://www.foreignpolicy.com/articles/2014/05/31/our_spying_is_better_than_your_spying, June 3, 2014.

7 Internet Media Research Center of China, "The United States' Global Surveillance Record," Xinhua News Agency, May 26, 2014, available at:http://news.xinhuanet.com/2014-05/26/c_1110865223.htm, June 3, 2014.

8 Yi Wenli, " China-US Differences in Cyberspace and Their Cooperation Path" (in Chinese), *Contemporary International Relations* (Monthly), Beijing, July 2012 Issue, pp.28-33.

9 Li Guomin. "ICANN's Stewardship Transition Does not Mean Controlship Transition" (in Chinese), *Science and Technology Daily*, March 24, 2014.

10 Michael N. Schmitt ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, 2013.

11 Zhu Qichao, Huang Changyun & Zhang Huang, "A Summary of the Third International Symposium on National Security and Science/Tech Development Strategy" (in Chinese), carried in *Contemporary International Relations* (Monthly), Beijing, August 2013 Issue, pp.64-65; Qichao Zhu, *Cross-domain Security and Cross-domain Deterrence: An Analytical Framework to Understand the Cyber-related Issues in the Information Age*, The Third International Seminar on the Strategy of National Security and the Development of Science & Technology (the 3rd ISST), Changsha, China, June 17-18, 2013.

12 Wang Jisi, Kenneth Lieberthal, *Addressing U.S.-China Strategic Distrust* (Chinese Version), Beijing, Social Sciences Academic Press, 2013.

13 See *Complete Works of Karl Marx and Frederick Engels* (Chinese edition), Vol. 7, Beijing: People's Publishing house, 2005, p.557.

14 *The Comprehensive National Cybersecurity Initiative* was issued in January 2008 during the G. W. Bush administration. When Barak Obama took the Office, *The Cyberspace Policy Review* was finished in May 2009, and *International Strategy for Cyberspace* was brought forth in May 2011, and the US did enact *Department of Defense Strategy for Operating in Cyberspace* in July 2011, and so on.

15 Jin Canrong & Duan Haowen, "Dilemma and Resolution of the Current China-US Relations" (in Chinese), carried in *International Review*, Shanghai, January 2014.

16 Wang Xiaofeng, "Cybersecurity Issues in China-US Relations" (in Chinese), carried in *American Studies Quarterly*, Beijing, March 2013.

17 Jan Van Tol, Mark Gunzinger, Andrew Krepinevich & Jim Thomas, *Air-Sea Battle: A Point-of-Departure Operational Concept*, Report of the Center for Strategic and Budgetary Assessments, 2010.

18 Yin Shuguang, "Crowe Memorandum the Inappropriate," *Wen Wei Po*, Hong Kong, April 1, 2014.

19 David C. Gompert & Philip C. Sunders, T*he Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability*, Institute for National Strategic Studies, National Defense University, 2010; Greg Austin & Franz-Stefan Gady, *Cyber Détente between the United States and China,* report of East West Institute, June 2012.

20 Stephen Harner, "U.S. Policy, Not China, Is Driving the Asian Arms Race," April 6, 2014, available at: http://www.forbes.com/sites/stephenharner/2014/04/06/u-s-policy-not-china-is-driving-the-asian-arms-race/, April 24, 2014.

21 Many Chinese people always frown to the annual report delivered by the US-China Economic and Security Review Commission since 2000, contents in such reports are seen in a tone of

exaggerating China's threat. Since 2010, the US-China Economic and Security Review Commission inclined to hold hacking activities related to intellectual property theft supported by Chinese government. Such information can be seen in the report of "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" by Northrop Grumman Corporation in March 2012; The IP Commission Report issued by the Commission on the Theft of American Intellectual Property in May 2013; and Jon Lindsay and Tai Ming Cheung's article "The Greatest Transfer of Wealth in History? Exploring the Relationship between Chinese Cyber Espionage and Technological Innovation" delivered on their website in July 2013.

22 Huang Changyun, Zhu Qichao & Zhang Huang, "Cyber Deterrence in the Cloud Computing View" (in Chinese), *National Defense Science and Technology*, Changsha, April 2013.