1

China's Internet Development and Cybersecurity – Policies and Practices

1.1. Introduction

After land, sea, air and outer space, many people have dubbed cyberspace as the fifth domain for human activities, with multiple implications for a state. Put simply, the political, economic and security interests of a state are now increasingly connected with cybersecurity. However, the Internet is a double-edged sword, i.e. it brings about not only enormous benefits but also numerous risks, challenges and threats. Therefore, given the borderless, transnational and unique nature of cyberspace, it has become a new frontier for global governance.

China attaches great importance to Internet development and has made enormous progress in this regard. However, as a late comer to this field, China faces various challenges and has been one of the major victims of cyber-attacks. Looking into the future, China is willing to strive for a peaceful, secure, open and cooperative cyberspace together with the international community.

Chapter written by Xu LONGDI.

Internationally, there are many doubts about China's policies and practices in its Internet development because of misunderstanding, prejudice, lack of knowledge, and even ignorance one the one hand. On the other hand, there is an increasing demand for understanding China's policies and practices in this domain. This chapter tries to introduce some of China's cyber policies and practices with a view to mitigating the doubts towards China.

This chapter is divided into six sections: the first section presents an overview of the development of Internet in China; the second section introduces China's policies towards Internet development; the third section elaborates on the cyber legislation and Internet administration in China; the fourth section examines China's idea on cyber diplomacy and its relevant activities and international cooperation concerning the Internet; the fifth section explores whether there is a cyberstrategy in China and its possible shape in the future. Finally, this chapter draws some temporary conclusions in line with the above analysis.

1.2. Internet development in China: an overview

Although China came relatively late to the Internet, the Chinese government and people warmly greeted the advent of the Internet era. During the mid- and late-1980s, China's researchers and scholars began to explore in an active manner the use of the Internet with the assistance of their foreign colleagues. On such occasions as the 1992 and 1993 INET annual conferences, Chinese computer specialists asked for Internet access for the Chinese public as a whole, which gained the understanding of and support from their international peers. During the China-U.S. Joint Committee of Science and Technology Cooperation meeting held in Washington in April 1994, the Chinese representatives ultimately reached a consensus with the U.S. National Science Foundation (NSF) on China's access to the Internet.

On 20 April 1994, the CAINONET for Education and Scientific Research in Zhongguancun district, Beijing was linked to the Internet via a 64k special line. This full-function connection marked China's formal access to the Internet.[1]

Since its inception in China, the Internet has witnessed a rapid and sound development. As of the end of December 2013, the number of Internet users in China has reached 618 million, a growth of 53.58 million over the end of 2012, according to the *33rd Statistical Report on Internet Development in China*[2] released by China Internet Network Information Center (CNNIC) in January 2014. The Internet penetration rate is 45.8%, a growth of 3.7% compared with that at the end of 2012. This figure indicates that the growth rate of the overall scale of Internet users in China has gradually slowed down since 2011.

In the meantime, the number of mobile Internet users has also experienced rapid growth. By the end of 2013, China had 500 million mobile Internet users, a growth of 80.09 million compared with that of 2012 and an annual growth rate of 19.1%. Among all the Internet users, the proportion of those using mobile phones to access the Internet rose from 74.5% to 81.0%, up by 6.5% over 2012. Mobile phones constituted the largest Inter-accessing terminal for the Chinese Internet users. The ratio of Internet users using desktops and laptops dropped slightly to 69.7% and 44.1% by 0.8% and 1.8% respectively, compared with the figure of 2012.

---

1 State Council Information Office, *White Paper on the Status of China's Internet*, 8 June 2010; 国务院新闻办公室：《中国互联网状况》白皮书，2010年6月8日。http://www.scio.gov.cn/zfbps/ndhf/2010/201006/t662572.htm.

2 China Internet Network Information Center (CNNIC), *The 33rd Statistical Report on Internet Development in China*, January 2014; 中国互联网络信息中心：《第33次中国互联网络发展状况统计报告》，2014年1月。http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201403/P020140305346585959798.pdf.

The rural Internet users had accounted for 28.6% of the total in China, reaching 177 million, a growth of 21.01 million over 2012.

China had a total of 18.44 million domain names, which included 10.83 million ".CN" domain names, up by 44.2% compared with that of 2012, accounting for 58.7% of the total domain names in China.

The total number of websites in China rose to 3.20 million, a growth of 520,000, up by 19.4% compared with that of 2012.

As of the end of 2013, 93.1% of Chinese enterprises use computers in their work, 83.2% use the Internet, 79.6% use broadband. In the meanwhile, the proportion of online marketing and online purchase conducted by the Chinese companies was 23.5% and 26.8% respectively, while that of using the Internet to conduct marketing and advertisement activities was 20.9%.

Along with the gradual slowing-down of the growth rate of the overall scale of the Chinese Internet users, the Internet in China is changing from a quantity-focused development model to a quality-focused one. In other words, the main thematic mission of the Internet in China has shifted from "increasing its penetration rate to deepening its utilization levels", which results from several factors, including changes in the policy environment. For instance, there has been increasing national policy support. In 2013, the State Council issued a policy paper "Opinions on Promoting Information Consumption to Expand Domestic Demand", which demonstrates the importance of the Internet in the Chinese economy and society. Moreover, the Internet is increasingly connected with traditional economy, for instance, it has witnessed very good applications in shopping, logistics, payment, and even finance. Furthermore,

the use of the Internet is gradually changing people's lifestyle, exerting influence upon almost every aspect of their daily life, including clothing, food, housing and transportation, and so on.

Of course, the development, spread and application of Internet in China also face various problems, such as regional imbalance as well as that between urban and rural areas. Constrained by such elements as economic development, education and overall level of social Informationization, China's Internet also takes on a unique feature, i.e. the Eastern part of China enjoys rapid Internet development while that of the Western part is slow, and the urban Internet penetration is high while that in the rural area is low. As of the end of 2009, Internet penetration in the Eastern part of China was 40.0%, while that of the Western part was 21.5%. In addition, there is also a big gap between urban and rural netizens, though the proportion of the latter has witnessed some increase from 27.8% in 2009 to 28.6% in 2013. Therefore, China still needs to make assiduous efforts to narrow the gap between different regions as well as that between urban and rural areas. The Chinese government will have to continue to promote Internet development and spread, thus making more people benefit from it.

1.3. China's policies towards Internet development

China sees Internet as a major opportunity for its reform, opening-up, and modernization cause. The Chinese government has formulated a series of policies, which map out the blueprints for its Internet development, clarify the priorities for different stages of Internet development, and promote the process of social informationization.

1.3.1. *From the very beginning of its development, China's Internet has been closely linked to the Chinese economy, and was programmed and integrated into its macro economic development blueprints*

For instance, as early as in 1993, China established the Joint Conference on National Economic Informationization, which shouldered the responsibility of taking a leading role in building the communication network on national public economic information.

In 1997, China drew up the National Informationization Program during the 9th Five-year Plan and Goals in 2010, which brought the Internet into the construction program of national information infrastructure and proposed to boost the process of national economic informationization by striving to develop the Internet industry.

Five years later in 2002, China promulgated its Specialized Informationization Planning Program during the 10th Five-year Plan on National Economic and Social Development, which set out the priorities for China's informationization development as practicing e-government, re-energizing software industry, strengthening the development and utilization of information resources, and accelerating the development of e-commerce, etc.

In December 2002, the 16th National Congress of the CPC proposed to drive industrialization through informationization and promote informationization through industrialization, thus opening a new way of industrialization.

In November 2005, China laid down its National Informationization Development Strategy 2006-2020, which was a long-term or strategic document on informationization development, further clarified the priorities for China's Internet development, and proposed to advance national

economic informationization centered on readjusting economic structure and transforming the economic growth model. The document also proposed to practicing e-government with improving governance capacity at its core, and to carry forward social informization centering on building a harmonious society, etc.

In March 2006, the National People's Congress (NPC) examined (deliberated) and approved the 11th Five-year Plan Outline on National Economic and Social Development, proposing to boost the merger of telecommunication network, broadcast network and Internet, and to build next-generation Internet and accelerate its commercial application.

In April 2007, a meeting of the CPC Political Bureau proposed to vigorously develop cyber culture industry and cyber culture information equipment manufacturing industry. In October 2007, the 17th National Congress of the CPC established the development strategy of "developing modern industry systems, strive to integrate Informationizationand industrialization, and promote the industries to transform from being big to being strong".

In January 2010, the State Council decided to speed up the merger of the telecommunication network, broadcast network and Internet and to advance the development of information and cultural industries.

Under the Chinese government's active promotion and explicit policy guidance, China's Internet has been gradually on a road of comprehensive, sustainable and rapid development.

1.3.2. *In addition to lending full policy support to Internet development, China also invests heavily in building Internet infrastructures*

From 1997 to 2009, China invested 4,300 billion RMB in Internet infrastructure construction nationwide, and completed communication optical fiber cable covering the whole country with a total length of 8.267 million kilometers, among which 840,000 kilometers are long-distance optical cable line. By the end of 2009, China's basic telecommunication companies possessed 136 million Internet broadband access (BBA) ports, with Internet international outlet bandwidth reaching 866,367 Mbps (million bits per second), having 7 log-in submarine cables and 20 land cables with a total volume of 1,600 Gb (Gigabyte).

99.3% of China's villages and towns, and 91.5% of its administrative villages enjoy access to Internet, while 96.0% of villages and towns have access to bandwidth network.

In January 2009, the Chinese government began to provide the 3G mobile communication licenses. Now, the 3G networks have fundamentally covered the whole country. The mobile Internet is experiencing rapid development, while the Internet will benefit more people.

1.3.3. *The Chinese government actively promotes the R&D of next-generation Internet (NGI)*

During the late 1990s, China began its work on the NGI R&D and implemented a series of major science and technology programs such as "new-generation highly reliable network". In 2001, the first Chinese NGI regional experimental network, near-field communication network (NFCNET), was established in Beijing. In 2003, China Next Generation Internet (CNGI) was officially launched and marked China's entrance into a new stage of large-scale NGI

R&D and construction. Now, China has established the world's largest IPv6 excellence network, while the medium- and small-capacity IPv6 router technology, authentication technology on authentic IPv6 source address and NGI transitory technology used in the experimental network are taking a lead internationally. The technological programs proposed by China on the internationalization of domain names, IPv6 source address authentication, IPv4-IPv6 transitory technology have gained the approval of the Internet Engineering Task Force (IETF) and become part of the international Internet standards and protocols.

1.3.4. *China practices a policy of managing cyber affairs in line with law, adhering to the principles of scientific and effective administration in its Internet governance*

It also endeavors to improve its Internet governance system, which is a combination of laws and norms, administrative supervision, industry self-discipline, public monitoring and social education. Since 1994, China has promulgated a series of laws and regulations related to Internet administration. To be sure, China will continuously improve its Internet governance through practices. China also advocates the free and secure flow of Internet information, which are not only the two sides of the same coin, but also constitute an indispensable and interdependent whole. It sticks to combat cybercrimes in accordance with the laws, and opposes any form of cyber hacker behaviors, which is in line with the spirit of the Chinese laws and regulations.

1.4. Cyber legislation and Internet administration

There is much misunderstanding about China's policies and practices on Internet governance and administration. In particular, after former U.S. Secretary of State Hillary

Clinton put forward the idea of cyber freedom in her Newseum speech in January 2010, there have been increasing accusations and criticisms against China in the media and news reports, though these allegations are inconsistent with the facts and sometimes prejudiced.

In fact, China adheres to the principle of scientific and effective Internet administration by law. After years of experience, China has formulated a system of Internet governance with different layers and types of laws and regulations in place. Of course, these laws and regulations conform to the specific national conditions in China. Different from some countries' one-sided emphasis on cyber freedom, China advocates the free and secure flow of information in cyberspace, which is just like the two wings of a bird.

Along with the rapid development and changes of ICTs, China also tries to keep with the times in its cyber legislation and Internet administration. On the one hand, it sometimes revises the established laws and regulations to make them fit the new ICT environment. On the other hand, the legislative body of China also makes new laws and regulations to tackle the new problems and new phenomena brought about by the Internet and ever-changing ICTs, in particular, to deal with those negative impacts upon the political, economic, social and cultural life of the Chinese people.

1.4.1. *Basic principles and practices of Internet administration in China*

According to the *White Book on the Internet in China*, the basic goals of China's Internet administration are: to promote general and hassle-free Internet accessibility, and sustainable and healthy development, guarantee citizens' freedom of speech online, regulate the order of Internet

information transmission, promote the positive and effective application of the Internet, create a market environment for fair competition, safeguard the citizens' rights and interests vested in the Constitution and law, and ensure safety for Internet information and state security.

In practice, China adheres to the principle of scientific and effective Internet administration by law. In general, China has formulated an effective and overall system of Internet administration, which is a combination of laws and regulations, administrative supervision, self-regulation, technical protection, public supervision and social education. In addition, China also strives to improve its Internet administration system constantly.

1.4.1.1. *Laws and regulations on Internet administration*

In line with the spirit of regulating the Internet by law, China has enacted a series of laws and regulations concerning Internet administration since 1994. They include:

– Decision of the National People's Congress Standing Committee on Strengthening the Protection of Internet Information (2012);

– Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000);

– Law of the People's Republic of China on Electronic Signatures (2004);

– Regulations on Telecommunications of the People's Republic of China (2000);

– Measures on the Administration of Internet Information Services (2000);

– Regulations on the Protection of Computer Information System Security of the People's Republic of China (1994 and revised in 2011);

– Regulations on the Protection of the Right to Online Dissemination of Information (2006);

– Provisions on the Administration of Foreign-funded Telecommunications Enterprises (2001 and revised in 2008);

– Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997);

– Provisions on the Administration of Internet News Information Services (2005);

– Provisions on the Administration of Electronic Bulletin Services via the Internet (2000);

and so on……

In addition, relevant provisions of other laws are also applicable in the case of Internet administration, such as:

– Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997);

– General Principles of the Civil Law of the People's Republic of China (1986);

– Copyright Law of the People's Republic of China (1990 and its second revision in 2010);

– Law of the People's Republic of China on the Protection of Minors (1991 and revised in 2006);

– Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006);

and so on……

These laws and regulations involve basic Internet resource management, information transmission regulation, information security guarantee and other key aspects. On the whole, they define the responsibilities and obligations of basic telecommunication business operators, Internet access

service providers, Internet information service providers, government administrative organs, Internet users and other related bodies.

1.4.1.2. *The leading role of the Chinese government in Internet administration*

The Chinese government plays a leading role in Internet administration. In accordance with their statutory duties, relevant government bodies are responsible for safeguarding Chinese citizens' rights and interests, public interests and state security by law. This is also true with the cyber field. Of course, as far as the Internet is concerned, there is a division of labor among these different governmental organs.

For example, *National telecommunications administration departments* are responsible for the administration of the Internet industry, including the administration of basic resources of the Internet, such as domain names and IP addresses within China.

There is a slight administrative difference between commercial and non-commercial Internet information services in China. According to the Measures on the Administration of Internet Information Services (2000), China carries out a licensing system for commercial Internet information services and a registration system for non-commercial Internet information services respectively.

In line with the above Measures, the *publication, education, health and other* administrative *departments* implement licensing systems for "Internet information services concerning press, publication, education, medical care, medicines and medical instruments".

Public security organs and other state law-enforcement agencies bear the responsibility for Internet security supervision and administration, and investigate and punish all types of network crimes.

1.4.1.3. *Industry self-regulation*

China advocates industry self-regulation and public supervision. The practice of self-regulation by the industry is a unique feature in China's Internet governance and administration. In this regard, some professional organizations, such as the Internet Society of China (ISC), play a leading role.

Founded in May 2001, ISC is a national organization of the Internet industry with a purpose of serving the development of the Internet industry, netizens and governmental decisions. Since its foundation, the ISC has issued a series of self-disciplinary regulations, which greatly promote the healthy development of the Internet in China. These self-disciplinary regulations include:

– Public Pledge of Self-regulation and Professional Ethics for the China Internet Industry (2002);

– Provisions of Self-regulation on Not Spreading Pornographic and Other Harmful Information for Internet Websites (2004);

– Public Pledge of Self-regulation on Anti-malicious Software (2006);

– Public Pledge of Self-regulation on Blog Service (2007);

– Public Pledge of Self-regulation on Anti-Internet Virus (2009);

– Declaration of Self-regulation on Copyright Protection of China's Internet Industry (2005);

and so on……

These public pledges of self-regulation do not have legally binding power as it is up to the participants to abide by the rules, carry forward good practices while resisting and shunning away from the bad ones. Though some Western

media reports are rather caustic about this practice of self-regulation, these self-disciplinary pledges do have a kind of soft power and play a role in setting examples of good practices and shaping a clean, sound, and healthy Internet environment in China. Thus, these public pledges of self-regulation constitute a complement to the legally binding laws and regulations. For example, through the practice of self-regulatory pledges, the ISC has made unremitting efforts in helping to counter spam, reducing the global spam percentage of Chinese e-mails from 23% in 2002 to 4.1% in 2009.

1.4.1.4. *Public supervision through special websites*

With a view to strengthening public supervision of Internet services and maintaining a clean and healthy Internet environment, China has established a lot of public reporting and reception organizations since 2004. They include:

– China Internet Illegal Information Reporting Center (CIIRC)[3];

– Internet Crime Reporting Center[4];

– 12321 Harmful and Spam Internet Information Reporting and Reception Center[5];

– 12390 Pornography Crackdown and Press and Publication Copyright Joint Reporting Center[6];

and so on……

In January 2010, China also issued the Measures for Encouraging the Reporting of Pornographic and Vulgar Information on the Internet and Mobile Media. In the future,

3 http://ciirc.china.cn/.
4 http://www.cyberpolice.cn/wfjb/.
5 http://www.12321.cn/.
6 http://www.shdf.gov.cn/.

these Internet industry self-disciplinary organizations will continue to play their due role in safeguarding Internet security. The Chinese government will also further support their work in this regard and protect the public's legitimate rights to online reporting of illegal information and acts.

Moreover, China also adheres to rational and scientific law-making, and reserves space for Internet development. As the ICTs change quickly, and new cyber risks and threats are also in constant flux, the governments in the world will always be under some kind of pressure for keeping up with these changes in their cyber legislations, in order to make their laws and regulations relevant and to better protect people's interests in cyberspace. China will also revise old laws and regulations on Internet governance and enact new ones in line with the changing landscape of the ICTs and cyber risks.

1.4.2. *Guaranteeing the free and secure flow of information in cyberspace*

As mentioned above, China advocates the free and secure flow of information in cyberspace. In fact, in the Chinese philosophy, cyber freedom and cybersecurity are interwoven with and complementary to each other. Without security, the free flow of information will lose its meaning as it might be obtained and even abused by anyone else. In a similar vein, without the free flow of information, the secure flow of information will also lose its value, because, to keep the information flow secure, it will be subject to certain security measures that might undermine its availability to a wide audience. Though there is neither absolute cyber freedom nor absolute cybersecurity in cyberspace, an appropriate balance between the two have to be vigorously sought. This is what China tries to do in its cyber policies, in particular, in its cyber legislations.

1.4.2.1. *Guaranteeing Citizens' Freedom of Speech on the Internet*

The White Book on the Internet in China states that the Internet has experienced full-scope application in the news communication field of China. The Chinese government encourages and supports the development of Internet news communication undertakings, provides the public with a full range of news, and at the same time guarantees the citizens' freedom of speech on the Internet as well as the public's right to know, to participate, to be heard and to oversee in accordance with the law.

1.4.2.1.1. Constitutional guarantee

Accordingly, Chinese citizens fully enjoy freedom of speech on the Internet. The Constitution of the People's Republic of China confers on Chinese citizens the right to free speech. Therefore, with their right to freedom of speech on the Internet protected by the law, they can voice their opinions in various ways on the Internet. One of the most prominent features of China's Internet development is the vigorous online exchanges of ideas.

For example, the huge quantity of BBS posts and blog articles is far beyond that of any other country in the world. In recent years, such newly-emerging online services as blog, micro-blog, video-sharing and social networking websites are developing rapidly in China and provide greater convenience for Chinese citizens to communicate online. Now, new Internet applications and new online services, including online finance, big data and cloud computing, have provided a broader scope for people to express their opinions.

1.4.2.1.2. Public supervision via the Internet

The Chinese government has also actively created conditions for the people to supervise the government, and attaches great importance to the Internet's role in

supervision. To put it simply, the Internet's role in supervision has been brought into full play in China.

In order to facilitate the public's reporting of corrupt and degenerate officials and suchlike, the central discipline inspection and supervision authorities, the Supreme People's Court (SPC), the Supreme People's Procuratorate (SPP) and other relevant bodies have set up informant websites. The informant website of the Central Commission for Disciplinary Inspection (CCDI) of the Communist Party of China (CPC) and the Ministry of Supervision, and the website of the National Bureau of Corruption Prevention are playing an important role in preventing and punishing corruption and degeneration among officials.

1.4.2.1.3. CCDI website for public supervision

Now, the Chinese government is actively using the practice of online reporting to fight against corruption, which has greatly facilitated the government's efforts in cracking down corrupt practices and officials. For example, CCDI established and opened a website[7] in September 2013 designed to publish information, elaborate policies, solicit public opinion, and promote anti-corruption efforts through online reporting. It has a special website[8] for online reporting of corrupt practices and officials. The CCDI website also has an interactive column, which contains online interviews and a message board. In particular, the interactive column will pose one question per month to solicit visitors' opinions on certain issues. So far, for example, they include:

– How to use the Internet to carry out anti-corruption efforts (September 2013);

7 http://www.ccdi.gov.cn/.
8 http://www.12388.gov.cn/.

– How to fight against "tigers" (high-ranking officials) and "flies" (low-ranking officials) (October 2013);

– How to deal with the relationship between abiding by the law on the one hand and treasuring personal relations or feelings (worldly wisdom), in the context of fighting against the four undesirable work styles (formalism, bureaucratism, hedonism, and extravagance) (November 2013);

– What is your opinion on utilizing critical time nodes and "trifles" to firmly redress the four undesirable work styles (December 2013);

– What is your advice on making the CCDI website perform better in the new year (January 2014);

– How to achieve the goal of fighting against corruption with "zero-tolerance" (February 2014);

– What else should be done to redress the four undesirable work styles, and how (March 2014);

– Please expose the stealthy or covert forms of the four undesirable work styles (April 2014).

These questions have always been followed by numerous messages left by the visitors to the website, which greatly facilitate the anti-corruption efforts of the Chinese governments.

In addition, other Chinese governmental departments have also set up their own website for online reporting. For instance, the Central Organization Department of the CPC has established a 12380 online reporting website[9], which is also a kind of online supervision over governmental officials.

9 http://www.12380.gov.cn/.

On November 21, 2013, the Supreme People's Court (SPC) of China created official accounts on Sina Weibo and WeChat, two of the country's leading social media tools, marking its efforts to promote judicial transparency. A statement from the SPC website said the new media accounts signal the SPC's steps to boost openness, value public opinions and widen the channel for the masses to oversee judicial authorities, which are in line with the spirit of the Third Plenary Session of the 18th Communist Party of China (CPC) Central Committee held in November 2013. The Chinese Netizens hailed it as "a milestone for China's rule of law" in the comments posted on the court's micro-blog account.

The above efforts and practices reflect not only the increasing openness and transparency of the Chinese government in its daily work, but also its willingness to solicit good opinions and advice from the people, much larger in number than that of governmental officials, to improve its daily work and even work styles. Now, the opinions expressed by the public online are receiving unprecedented attention. In other words, the Internet has become a new channel for the Chinese government to get to know the people's situation and amass the public's wisdom, and consequently exercise governance for the people and improve its work.

To quote the *White Book on the Internet in China*, the Internet provides unprecedented convenience and a direct channel for the people to exercise their right to know, to participate, to be heard and to oversee, and is playing an increasingly important role in helping the government get to know the people's wishes, meet their needs and safeguard their interests. In a word, the Chinese government is determined to unswervingly safeguard the freedom of speech on the Internet enjoyed by Chinese citizens in accordance with the law.

1.4.2.1.4. Protecting citizens' online privacy

As more cases of Internet users' information being leaked are emerging, the protection of citizens' online privacy is becoming high on the Chinese government's agenda, because it is closely connected with the people's sense of security and confidence in the Internet. In fact, there are already provisions in the existing Chinese laws and relevant regulations.

For instance, the Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000) stipulates that illegal interception, tampering with or deletion of others' e-mails or other data and infringement upon citizens' freedom and privacy of correspondence that constitutes a crime shall be investigated for criminal liability in line with the Criminal Law.

Moreover, according to the self-disciplinary public pledges of the Internet industry (2002), Internet service providers are responsible for protecting users' privacy. The providers shall publish their relevant privacy protection commitment when providing services, provide reporting and reception channels for privacy infringement and take effective measures to protect users' privacy.

Of course, the Chinese government will always improve relevant legislation and Internet corporate service regulations, in order to steadily enhance online privacy protection systems.

1.4.2.1.5. Guaranteeing online safety for minors

Minors have become China's biggest online group. Therefore, the Chinese government attaches great importance to online safety for minors, and has always prioritized the protection of minors in the overall work of Internet information security programs.

The Law of the People's Republic of China on the Protection of Minors (1991 and revised in 2006) stipulates that the state shall take measures to prevent minors from overindulging in the Internet and to prohibit any organization or individual from producing, selling, renting or providing by other means electronic publications and Internet information containing pornography, violence, murder, terror, gambling or other contents harmful to minors.

In recent years, more and more people and organizations in China are calling for special laws and regulations concerning guaranteeing the online safety for minors. In particular, China advocates that families, schools and all other social units shall work together to protect minors online and create a healthy online environment for the development of minors.

From late September to November 2013, the State Internet Information Office (SIIO), the Ministry of Education (MOE), the Central Committee of the Communist Youth League of China and the All-China Women's Federation (ACWF) jointly initiated a two-month campaign dubbed "Green Web" to tighten supervision of websites and cell phone applications to fight lewd content and aggressive remarks aimed at young people. A statement released by the SIIO said that the move aims to further cleanse the Internet environment, provide a healthy and positive online environment for young people and protect their legal interests.

1.4.2.2. *Protecting Internet Security*

The White Book on the Internet in China says that Internet security is a prerequisite for the sound development and effective utilization of the Internet. The Chinese government holds that the Internet is an important national infrastructure. Therefore, within Chinese territory, the

Internet is under the jurisdiction of Chinese sovereignty, and the Internet sovereignty of China should be respected and protected. Accordingly, citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and protect Internet security.

First, China protects Internet security in accordance with the law. Numerous related rules are included in the existing Chinese laws and regulations in order to promote the sound development of China's Internet, protect state security, social and public interests, and lawful rights and interests of individuals, legal persons and other organizations. These laws and regulations include:

– Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997);

– Decision of the National People's Congress Standing Committee on Strengthening the Protection of Internet Information (2012);

– Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000);

– Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006);

– Regulations on Telecommunications of the People's Republic of China (2000);

– Regulations on the Protection of Computer Information System Security of the People's Republic of China (1994 and revised in 2011);

– Measures on the Administration of Internet Information Services (2000);

– Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997);

and so on……

For instance, Article 6 of the Regulations on Telecommunications of the People's Republic of China (2000) stipulates that "the security of telecommunications networks and information shall be protected by law. No organization or individual may utilize telecommunication networks to engage in activities that jeopardize state security, the public interest or the legitimate rights and interests of other people".

Second, China protects the secure flow of information. China believes that the free and secure flow of Internet information is an integral whole. To put it differently, on the premise of protecting the safe flow of Internet information, the free flow of Internet information may be realized. Therefore, the Chinese government attaches great importance to protecting the secure flow of Internet information, actively guides people to manage websites in accordance with the law and use the Internet in a wholesome and correct way.

The Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000), Regulations on Telecommunications of the People's Republic of China (2000), and Measures on the Administration of Internet Information Services (2000) contain clear stipulations that no organization or individual may produce, duplicate, announce or disseminate information having the following contents:

– being against the cardinal principles set forth in the Constitution;

– endangering state security, divulging state secrets, subverting state power and jeopardizing national unification;

– damaging state honor and interests;

– instigating ethnic hatred or discrimination and jeopardizing ethnic unity;

– jeopardizing state religious policy, propagating heretical or superstitious ideas;

– spreading rumors, disrupting social order and stability;

– disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime;

– humiliating or slandering others, trespassing on the lawful rights and interests of others;

– other contents forbidden by laws and administrative regulations.

It is noteworthy that these regulations are the legal basis for the protection of Internet information security within the territory of the People's Republic of China. In addition, all Chinese citizens, foreign citizens, legal persons and other organizations within the territory of China must obey these provisions.

Third, China opposes all forms of computer hacking. China is one of the countries suffering most from hacking. Like other countries, China faces a severe challenge of online criminal activities such as computer hacking and viruses. Chinese laws prohibit all forms of hacking compromising Internet security.

For example, the Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000) stipulates that acts deconstructing Internet security which constitute crimes, such as "intentionally inventing and spreading destructive programs such as computer viruses to attack the computer system and the communications network, thus damaging the computer system and the communications network", shall be

investigated for criminal liability in accordance with the relevant provisions in the Criminal Law.

Likewise, Articles 285 and 286 of the Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997) contain concrete provisions on the criminal punishment of illegal activities such as illegally obtaining data stored in or handled or transmitted by the computer information system, or providing destructive programs or tools for invasion and illegal control of computer information systems.

Fourth, China combats computer crime in accordance with the law. In recent years, computer crimes in China have been on the increase. Online fraud, online theft and other forms of crimes encroaching on the property of others are increasing rapidly. In order to effectively combat computer crimes, the Chinese laws stipulate that criminal activities conducted by making use of the Internet or against the Internet shall be investigated and dealt with in accordance with the Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997); if such activities are not serious enough to constitute crimes, administrative punishment shall be meted out in accordance with the Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006) and Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997).

On the operational level, the Ministry of Public Security (MPS) has established a Bureau for Cybersecurity Protection, which is especially devoted to combating cybercrimes. It also conducts international cooperation in this regards. For instance, China and the United States have carried out cooperation in fighting against cybercrimes.

In brief, cyber freedom and cybersecurity are the two sides of the same coin. In general, the Chinese government has actively explored channels and methods of scientific and effective Internet administration by law, and has formed a preliminary Internet administration model that is suitable for China's conditions and consistent with international practices. Of course, Internet administration is a process of continuous practice, and the Chinese government will further improve its efforts on Internet administration.

1.5. Cybersecurity and diplomacy: an international perspective

In an interconnected cyber world, there is neither absolute security nor absolute freedom for anyone or any state. In other words, any country could not go it alone in the interdependent cyber world. In another sense, though connected, the Internet of various countries belongs to different sovereignties, which also makes it necessary to strengthen international exchanges and cooperation in this field. Therefore, cyber cooperation is of both practical and strategic necessity. In the future, all countries should enhance international and bilateral cyber exchanges and cooperation, learn more about each other's concerns, and build mutual trust in order to build a peaceful, secure and open cyberspace.

According to the *White Book on the Internet in China*, China maintains that all countries should, on the basis of equality and mutual benefit, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security, promote the healthy and orderly development of the industry, and share the opportunities and achievements brought about by this development.

In practice, China has promoted international cooperation on cyber issues in an active manner. By now, it has conducted various strategic and security dialogues and consultations on cybersecurity with numerous countries, carried out legal cooperation on fighting against cybercrimes, engaged in technical cooperation in addressing cyber incidents on a daily basis, and so on. All these are signs of China being sincere, open and practical to international cybersecurity dialogue and cooperation. To put it simply, international cooperation on cybersecurity has become an inherent part of China's policies, practices and even strategy.

1.5.1. *Cyber policy dialogue and consultation*

China actively promotes the establishment of bilateral dialogue and exchange mechanisms in the field of the Internet, through which China and relevant countries exchange their policies and practices on the Internet development and cybersecurity, know more about and learn from each other, increase mutual understanding, build confidence and mutual trust, thus contributing the Internet development and cybersecurity.

For example, in their Strategic Security Dialogue under the framework of China-U.S. Strategic and Economic Dialogue (S&ED), China and the United States have touched upon and begun to talk about cybersecurity issues. During U.S. Secretary of State John Kerry's visit to Beijing in April 2013, the two sides decided to set up a working group on cybersecurity within the framework of the China-U.S. S&ED. In their meeting, Chinese Foreign Minister Mr Wang Yi told Kerry that China and the United States should make joint efforts to safeguard cyberspace, which should be an area where the two countries can increase mutual trust and cooperation.

The first China-U.S. cybersecurity working group meeting was held on July 8, 2013 in Washington, ahead of the 5th round of the China-U.S. S&ED taking place on July 10-11, 2013. Under the context of whistleblower Edward Snowden's revealing of the bulk Internet and telephone surveillance over American and non-American citizens conducted by the U.S. National Security Agency (NSA), the cybersecurity issue undoubtedly became a hot topic during the S&ED.

The two sides held candid and in-depth exchanges on the improvement of the cyber working group mechanism, cyber ties between the two countries, international cyberspace regulations and a bilateral dialogue on and cooperation in cybersecurity. China and the U.S. reportedly hope to create the mechanism under the principals of mutual respect and equal dialogue, so that the working group can play a positive role in enhancing mutual trust, reducing differences and expanding cooperation in cybersecurity. The two sides also agreed to hold another meeting within the year.[10]

On December 3, 2013, the working group held another meeting in Beijing, during which the two sides held a candid, in-depth and constructive dialogue and reached good results. They thought positively of the relevant exchanges and cooperation in the cyber field between the two sides since their first meeting in July 2013. They also expressed their willingness to strengthen the dialogue and cooperation, and to manage and control their disputes, with a view to promoting the sound interaction in the cyber field between the two sides, on the basis of mutual respect and win-win

10 Zhang Ming'ai, "Cybersecurity tops China-US S&ED agenda", July 10, 2013, http://www.china.org.cn/world/2013-07/10/content_29382578.htm

cooperation. Officials and experts from numerous departments of the two countries attended the meeting.[11]

China has also held cybersecurity dialogues and consultations with France, Germany, South Korea, the European Union, and other countries and organizations in recent years. Moreover, as of the end of 2013, the State Council Information Office and the State Internet Information Office of the People's Republic of China have hosted China-U.S. Internet Industry Forum (6 times) and China-UK Internet Roundtable (5 times), China-South Korea Internet Roundtable (2 times) with the United States, the United Kingdom and the Republic of Korea respectively since 2007.

To draw on the experience of other countries in developing and administering the Internet industry, the Chinese government has organized dozens of delegations since 2000 to visit dozens of countries in Asia, Europe, North America, South America and Africa, and has learnt and applied some of their successful experiences to its own Internet development and administration.

1.5.2. *Regional cyber cooperation*

China attaches great importance to regional cooperation in maintaining Internet security. As early as in 2009, China signed the China-ASEAN Coordination Framework for Network and Information Security Emergency Responses,

11 On the Chinese side, they include the Ministry of Foreign Affairs, the Ministry of National Defense, the Ministry of Public Security, the Ministry of Industry and Information Technology, the State Council Information Office. On the American side, they include the Department of State, the National Security Council of the White House, the Department of Defense, the Department of Homeland Security, Department of the Treasury, and FBI. See "China-U.S. Working Group on Cybersecurity holds a meeting in Beijing", December 4, 2013, http://www.fmprc.gov.cn/mfa_chn/wjb_602314/zzjg_602420/bmdyzs_602866/xwlb_602868/t1105394.shtml.

and the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, with the ASEAN and SCO member states respectively.

In September 2013, China hosted an "ASEAN Regional Forum (ARF) Workshop on Measures to Enhance Cybersecurity – Legal and Cultural Aspects" in Beijing, trying to build regional consensus and work out practical measures on cybersecurity. China also participate in the work and activities on cybersecurity within the framework of the Council for Security Cooperation in the Asia-Pacific (CSCAP), Asia-Pacific Economic Cooperation (APEC), and the Conference on Interaction and Confidence-Building Measures in Asia (CICA), etc.

On April 2, 2014, China issued a policy paper on the European Union (EU)[12], which contains both the macro goals and the micro measures on promoting China-EU cooperation on cybersecurity. On the macro level, it states that China and the EU should "strengthen cybersecurity dialogue and cooperation and promote the building of a peaceful, secure, open and cooperative cyberspace", and "facilitate practical cooperation between China and the EU in fighting cyber-crimes, emergency response to cybersecurity incidents and cyber capacity building through platforms such as the China-EU Cyber Taskforce and work together for the formulation of a code of conduct in cyberspace within the UN framework".

On the operational level, it says that the two sides should "strengthen China-EU Dialogue on Information Technology, Telecommunication and Information, conduct exchanges and dialogue on related strategies, policies and regulations and

12 "China's Policy Paper on the EU: Deepen the China-EU Comprehensive Strategic Partnership for Mutual Benefit and Win-win Cooperation", April 2014, http://news.xinhuanet.com/english/china/2014-04/02/c_133230788_2.htm.

actively promote cooperation and exchanges on trade in IT products and industrial technology", "encourage broader exchanges on intellectual property rights and technical standards and continue to raise the level of China-EU cooperation on intellectual property rights", and "strengthen China-EU cooperation and exchanges on information security, especially cybersecurity".

1.5.3. *Track Ⅱ cyber diplomacy*

In addition to official exchanges and cooperation with other countries, China also carries out Track Ⅱ cyber activities. For instance, the Internet Society of China (ISC) and the U.S. think tank EastWest Institute (EWI) conducted a joint research and released a report on "Fighting Spam to Build Trust" in June 2011[13]. Two years later, the ISC and EWI presented another joint report *Frank Communication & Sensible Cooperation to Stem Harmful Hacking* at the EWI-IEEE World Cyberspace Cooperation Summit held at Stanford University in November 2013.[14]

Moreover, the China Institute of Contemporary International Relations (CICIR) and the Center for Strategic and International Studies (CSIS) of the United States have held seven formal meetings on cybersecurity (accompanied by several informal discussions) since 2009, called "Track Ⅱ China-U.S. cybersecurity Dialogue". According to the CSIS website introduction, the goals of the discussions have been to reduce misperceptions and to increase transparency of both countries' authorities and understanding on how each country approaches cybersecurity, and to identify areas of

13 "Fighting Spam to Build Trust", EastWest Institute and Internet Society of China, June 2011.

14 Karl Frederick Rauscher and Zhou Yonglin, *Frank Communication & Sensible Cooperation to Stem Harmful Hacking*, November 2013, http://www.isc.org.cn/download/China-U.S.%20Anti-Hacking%20Report.pdf.

potential cooperation, including confidence building measures and agreement on norms and rules for cybersecurity. The meetings have been attended by a broad range of Chinese and U.S. officials and scholars responsible for cybersecurity issues.[15]

1.5.4. *Legal cooperation in combating cybercrimes*

As cybercrimes have become increasingly rampant in recent years, and given the fact that cybercrime constitutes the bulk of malicious cyber activities, China has participated actively in international cooperation on combating cybercrime. According to the *White Book on the Internet in China*, in combating network crimes, the Chinese public security organ has participated in the Interpol Asia-South Pacific Working Party on IT Crime, China-US Joint Liaison Group (on Law Enforcement) and other forms of international cooperation, and has conducted bilateral and multilateral meetings successively with such countries or regions as the US, the UK, Germany, Italy and Hong Kong.

The Council of Europe Convention on Cybercrime or Budapest Convention on Cybercrime is a vanguard in combating cybercrimes.[16] The Convention plays a constructive role in promoting international judicial cooperation on fighting against cybercrimes. However, the Convention, which was formed in 2001, also has its inherent deficiencies, such as an inadequate voice and representation for the developing countries and therefore fails to adequately reflect the concerns of the developing world in fighting cybercrime. In particular, there is regulation about extraterritorial jurisdiction, which might constitute a

15 See CSIS website http://csis.org/program/china-institute-contemporary-international-relations-cicir.

16 See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

violation of state sovereignty and be incompatible with domestic legislations in case of a transnational collection of evidence. As a result, China has not signed it until now. However, it has participated in relevant activities concerning the Convention, expressed its views on relevant matters, and conducted wide-ranging practical communications with other countries and organizations on this. In other words, accession to it or not has not been a precondition for carrying out practical exchanges and cooperation on the ground. In essence, with or without it, there would be successful international cooperation on dealing with cybercrimes.

For example, China's Policy Paper on the EU discussed above states that China will "advance China-EU cooperation on police law enforcement, implement the five-year police training cooperation project, expand exchanges on policing administration, public security management, law enforcement regulation, criminal investigation technologies and the fight against organized crimes by organizing training courses, visits and seminars, increase the mutual trust between the two sides, and lay a solid foundation for jointly combating terrorism, economic, cyber and drug-related crimes, organized illegal immigration and other serious organized transnational crimes". This fully demonstrates the willingness and sincerity of China to engage in practical cooperation with other countries and organizations on fighting against cybercrimes.

In practice, the Chinese public security bodies handled from 2006 to 2009 more than 500 letters of assistance in case handling from more than 40 countries and regions concerning network crimes, which cover many types of cases, including hacker attacks, child pornography and network fraud.

1.5.5. *Technical cooperation*

On a technical level, it is easier for countries to cooperate with each other. The Ministry of Industry and Information Technology (MIIT) is the main governmental department responsible for IT research and development, relevant policies, and international technological cooperation, though other departments might also cover certain aspects of technical matters. Some major Internet security companies, such as China Mobile, China Unicom, China Telecom, and others also have an important role to play in China's Internet development and cybersecurity.

In addition, some professional organizations are inalienable for China's Internet security and international cyber cooperation, including the Internet Society of China (ISC), the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT/CC), and the China Internet Network Information Center (CNNIC), and so on.

1.5.5.1. *CNCERT*

The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT or CNCERT/CC) is an organization of network security technical coordination. Since its foundation in September 1999, CNCERT has been dedicated to carrying out the work of preventing, detecting, warning and handling China network security incidents under the policy of "positive prevention, timely detection, prompt response, guaranteed recovery", to maintain the safety of China's public Internet and ensure the safe operation of the information network infrastructures and the vital information systems.

Branches of CNCERT have spread in all provinces, autonomous regions and municipalities in mainland China. As China's core technical coordination organization,

CNCERT is playing a vital role in coordinating all Computer Emergency Response Teams within the country to handle cybersecurity incidents jointly.

CNCERT is active in developing international cooperation and is a window for handling network security incidents with the world. As a full member of the famous international network security cooperative organization FIRST and one of the initiators of APCERT, CNCERT devotes itself to building a prompt response and coordination handling mechanism of cross-border network security incidents. By 2013, CNCERT had established "CNCERT International Partners" relationships with 127 organizations from 59 countries or regions.[17] Therefore, CNCERT engages in practical and technical cooperation with other countries in addressing cross-border cybersecurity incidents.

In addition to the International Partnership program, it has also officially signed memorandums of understanding (MOUs) on cybersecurity cooperation or reached agreements with dozens of the above-mentioned organizations, and has gradually improved and enhanced the collaborative mechanisms on addressing cross-border cybersecurity incidents.

For instance, in 2012, it tackled 4,063 cybersecurity incidents involving elements within China (an increase of 3 times as many as that of 2011) in coordination with overseas security organizations, and assisted foreign agencies in addressing 961 cybersecurity incidents, an increase of 69.2% compared with that of 2011. These cybersecurity incidents included not only those DDoS attacks and phishing activities against China, but also those against foreign banks and companies, such as the Bank of America (BOA), the National Australia Bank, and PayPal. In October 2012, CNCERT received a complaint from the USCERT, which claimed that

17 http://www.cert.org.cn/publish/english/index.html.

some of the host computers located in China were controlled by malwares and participated in DDoS attacks against certain US banks and companies, and asked China for assistance in dealing with them. After some examinations, CNCERT addressed 75 IP addresses, provided by the USCERT, in a timely manner. Moreover, CNCERT also cracked down on a botnet named Nitol together with the Microsoft Corporation, in which the domain name 3322.org, used to spread and control malwares, was eliminated and more than 70,000 malicious domain names were closed.[18]

CNCERT also publishes weekly, monthly and annual reports on cyber threats and the cybersecurity situation in China, from which we can see that every week it deals with dozens or even hundreds of transnational cyber incidents together with its counterparts from other countries. It also participates in APCERTS' annual exercises, provide relevant training courses and programs to ASEAN members, engage in bilateral and multilateral cooperation with other countries and regional and international organizations, thus greatly facilitating and contributing to the Internet security all over the world.

1.5.5.2. *CNNIC*

The China Internet Network Information Center (CNNIC) is an administration and service organization that was set up on June 3, 1997 upon the approval of the competent authority which undertakes the responsibilities as the national Internet network information center.

---

18 National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cybersecurity Posture in 2012*, 19 March 2013; 国家互联网应急中心：《2012年我国互联网网络安全态势综述》，2013年3月 http://www.cert.org.cn/publish/main/46/2013/20130320093925791767941/20130320093925791767941_.html.

Its overall task is to "provide efficient and application-oriented services through secure and stable Internet infrastructure for public interests". As an important constructor, operator and administrator of infrastructure in Chinese information society, CNNIC is responsible for the operation, administration and services of fundamental Internet resources. It also undertakes R&D and security work of fundamental Internet resources, conducts research on Internet development and provides consultancy, and promotes the cooperation and technological exchange of global Internet in an effort to become an excellent network information center.

Its main responsibilities[19] include: (1) operation, administration and service organization of national network fundamental resources[20]; (2) research, development and security center of national network fundamental resources[21]; (3) research and consulting service driving force for Internet

19 See http://www1.cnnic.cn/AU/Introduction/Introduction/201208/t20120815_33295.htm.

20 CNNIC is a registry of domain names and root zone operator. It operates and administers country code top level domain of .CN and Chinese domain name system, and provides 24-hour services of domain name registration and resolution as well as WHOIS lookup for worldwide users with its professional technologies. CNNIC is a member of Asia-Pacific Network Information Center (APNIC) as a National Internet Registry (NIR). As the convener of IP Address Allocation Alliance, CNNIC is responsible for providing allocation and administration services to China's Internet service providers (ISPs) and Internet users and promoting the transition to Internet of next-generation based on IPv6 in China.

21 CNNIC constructs a world-leading, efficient and safe & stable service platform for fundamental network resources. It provides multi-level and multi-mode not-for-profit services for fundamental network resources, and seeks to make a breakthrough in the core competence of fundamental network resources and self-developed devices and softwares so as to improve the reliability, security and stability of China's system of fundamental network resources.

development[22]; (4) platform for Internet open cooperation and technical exchange.

In particular, CNNIC tracks the latest development of Internet policies and technologies and has business coordination and cooperation with relevant international organizations and the Internet network information centers in other countries and regions. In addition, CNNIC hosts important international conferences and activities concerning the Internet, and creates an open research environment and platform for international exchange and sharing. In this way, it promotes the application of scientific research achievements and development of China's Internet.

1.5.5.3. *ISC*

The Internet Society of China (ISC) was inaugurated on May 25, 2001. It is sponsored by more than 70 sponsors, including network access carriers, ISPs, facility manufacturers and research institutes, etc. It has more than 400 members covering legal companies, research institutes, academic associations, universities and other organizations engaged in various activities related to the Internet. The main mission of ISC is to promote development of the Internet in China and make efforts to construct an advanced information society. ISC is also expected to be a link among the community to make efforts benefiting the whole industry, to push forward industry self-discipline, to strengthen communication and cooperation between its

22 CNNIC is responsible for conducting surveys about the Internet including surveys on the development status of China's Internet, and it gives a description of the macroscopic picture of the development status of China's Internet and records its development faithfully. CNNIC will continue to beef up its support for the research of government policies on the one hand and provide not-for-profit research and consulting services for Internet development for enterprises, users and research institutes on the other hand.

members, to assist and provide support for making policies, and to promote Internet application and public awareness.[23]

1.5.6. *Office for Cyber Affairs of the MFA*

To deal with increasingly prominent cybersecurity issues and enhance intra-governmental coordination on the external aspects of cyber affairs, the Ministry of Foreign Affairs established the Office for Cyber Affairs in June 2013, whose responsibility is to coordinate and conduct diplomatic activities related to cyber affairs.[24] Then, Mr. Fu Cong, a counselor from the Department of Arms Control of MFA was appointed as the Coordinator for Cyber Affairs. Mr. Fu has rich diplomatic experiences. He once served as an adviser to the Director-General of the World Health Organization (WHO).[25]

Though the MFA does not enjoy an advantage over technological details, it has rich experiences in dealing with international affairs. As the Internet has a transnational feature, as ICTs can be commanded by anyone with some

23 About Internet Society of China, see http://www.isc.org.cn/english/About_Us/Introduction/.

24 http://www.fmprc.gov.cn/mfa_chn/wjdt_611265/fyrbt_611275/t1050377.shtml.

25 Fu Cong, a Chinese national, is adviser to the Director-General. His diplomatic career began when he joined the Chinese Foreign Ministry in 1987. He has served in posts based in Beijing and overseas in Geneva and Vienna. He became Deputy Director General of the Arms Control Department of the Chinese Foreign Ministry in 2003, and was the Deputy Director General of the Foreign Affairs Office of China's Xinjiang Autonomous Region from 2004-2005. From September 2005 to October 2007, Mr. Fu worked as a minister-counselor in China's Permanent Mission in Geneva. He worked on many issues, including those related to the international organizations based in Geneva, including WHO, the World Intellectual Property Organization and the International Telecommunication Union. Mr. Fu graduated from the Foreign Affairs College in Beijing, China and studied at the Polytechnic of Central London in the United Kingdom. He is married with one child. See http://www.who.int/dg/office/cong/en/index.html.

computer expertise or skills, as cyber threats and cybercrimes do not respect sovereign borders, every Foreign Ministry in the world could play an important role in coping with the international aspects of cyber issues, in addressing trans-border cyber risks, threats, and incidents, in fighting against cybercrimes, in engaging in international cooperation, building mutual trust, and maintaining international order in cyberspace.

Therefore, it is expected that the Office of Cyber Affairs under the MFA of China will also play its due roles in cyber issues. One the one hand, it could present China's ideas, visions and interests to the outside world; on the other hand, as its mission states, it could coordinate and conduct diplomatic activities related to cyber affairs.

All of the above are signs of China being open and cooperative in the cyber field and constitute a starting point for future international cooperation with a view to building a peaceful and secure cyberspace for all.

1.6. A cybersecurity strategy in the making?

In recent years, the number of cyber-attacks has increased significantly, the occurrence of cyber incidents has become more frequent, and cyber-attacks *per se* have become increasingly complex. As a result, more and more countries have become some kind of victims of cyber-attacks on the one hand, and have realized the seriousness of cyber-attacks and the importance of cybersecurity on the other hand. Therefore, numerous countries have published their cybersecurity strategies, which usually acknowledge both the benefits and damages that the Internet has brought about to humankind and people's daily life, clarify the goals and objectives they want to achieve in cyberspace, and define the means of tackling cyber threats and safeguarding cybersecurity.

Under this context, many people have asked whether China has a cybersecurity strategy and, if not, whether China should have such a strategy and when China will have such a strategy. With regard to the former, literally, the answer is no. So far, China has not published such a policy paper as a cybersecurity strategy. However, the Information Office of the State Council did published a *White Paper on the Internet in China* in June 2010, which is a comprehensive introduction about the development of the Internet in China, as well as China's policy and practices on cyber issues.

As for the latter, though there is not an assured answer to the "when" question, the answer to the "whether" question would be yes for several reasons. First, in recent years, China has also suffered from increasing cyber-attacks, and it needs a strategy to deal with those various cyber threats. Second, as more and more countries in the world have produced their cybersecurity strategies, China is also under a kind of international peer pressure to have one of its own making. Third, just like other countries, different governmental departments are in charge of different aspects of ICT issues, such as Internet development, information and communication technologies, and international exchanges, though there are some overlaps with regard to some of their functions. So, there is a lack of a central and coordinating body covering the full-spectrum of cybersecurity issues. To put it differently, there is a question of "calling whom" when a cyber incident occurs or submitting a report to whom when there are some reports and suggestions regarding cyber affairs.

As a matter of fact, there are many voices in China calling for the government to produce a cybersecurity strategy and establish a special administrative organization to coordinate and manage those issues connected with cybersecurity. For instance, the National Computer Network Emergency

Response Technical Team/Coordination Center of China (CNCERT/CC) puts forward such advice almost every year in its annul reports on China Cybersecurity Posture.[26] Many scholars also have similar ideas in their academic writings and reports. Now, their efforts begin to yield results.

Facing the increasingly severe cybersecurity situation, the Chinese government has sensed the need to increase the coordination between different governmental departments, different sectors, and different layers of work in the field of ICT. Now, the highest authority begins to take action. On February 27, 2014, the Central Leading Group on Internet Security and Informationization held its first meeting in Beijing.

According to a statement released after the first meeting of the group, President Xi Jinping will head the central Internet security and informatization leading group. Premier Li Keqiang and Liu Yunshan, who are both members of the Standing Committee of the Political Bureau of the Communist Party of China Central Committee, are the group's deputy heads. Members of the group also adopted the group's work rules and its working plan for this year at the meeting.

President Xi presided over the meeting, stressing that Internet security and informatization is a major strategic issue concerning a country's security and development as well as people's life and work. He said that "efforts should be made to build our country into a cyber power". Therefore, the group is designed to lead and coordinate Internet security

26 National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cybersecurity Posture in 2012*, 19 March 2013; 国家互联网应急中心：《2012年我国互联网网络安全态势综述》，2013年3月。http://www.cert.org.cn/publish/main/46/2013/20130320093925791767941/20130320093925791767941_.html.《2013年我国互联网网络安全态势综述：CNCERT观点》。

and informatization work among different sectors, as well as draft national strategies, development plans and major policies in this field.

The president also noted that China has the world's largest number of Internet users but still lags behind in the development of Internet technologies. In addition, the digital gap between rural and urban areas remains large and the average bandwidth enjoyed by each Chinese person is far less than that in some developed countries. For instance, by the end of 2013, China reported about 618 million Internet users, but only 28.6 percent of them live in the countryside. President Xi emphasized that "we should be fully aware of the importance and urgency of Internet security and informatization". The president also said that China has to balance its needs of developing IT technologies and safeguarding Internet security, describing the two issues as two wings of a bird and two wheels of an engine.[27]

Now that the Central Leading Group on Cybersecurity and Informationization has been established and convened its first-ever meeting, we believe that it will play an increasingly important and substantial role in coordinating cybersecurity affairs on the highest level of authority in the future.

With the Central Leading Group now being in place, it is expected to carry out its functions and duties as set out during its first meeting. In particular, it will play a bigger role in formulating cyber policies on the strategic level or of strategic significance. Accordingly, a Chinese version of cybersecurity strategy might emerge in the future.

27 "Xi heads Internet security group", xinhuanet, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148418.htm.

To put it literally, a strategy usually contains two basic components: one is to clarify and define the goals or objectives one wants to achieve, while the other is to find out and shape the means or ways of realizing the established goals and objectives. In essence, a strategy requires a match between the goals and means. If there is a mismatch, a strategy will run into problems.

As with other countries' cybersecurity strategies, the Chinese one will also include the following contents: to demonstrate the significance and meaning of Internet development for China, define cyber goals and objectives China wants to achieve in cyberspace, identify possible cyber risks and threats China might face, and figure out feasible policy measure.

1.6.1. *Significance of the Internet for China*

As argued above, there is no doubt that the Internet is of great significance for China's reform, opening up, development and modernization cause. This will also be the case for China in the future. Just like the United States, China will be another country in the world to have a high-degree of reliance upon the Internet and ICTs.

1.6.2. *Goals and objectives*

The overall goal of China's cyber policy is to maintain and build a peaceful, secure, open and cooperative cyberspace, for the benefits of both the Chinese people and humankind as a whole.

1.6.3. *Cyber threat landscape*

Just like the rapid development of ICTs *per se*, the threats, risks and vulnerabilities inherent in or accompanying ICTs also change continuously. Therefore, the

threat landscape will change constantly, which poses the biggest challenge for China's cybersecurity.

China has made great progress in developing its Internet, but as with others, it also faces various security challenges in cyberspace. In fact, China has been a major victim of cyber-attacks, which have been increasing dramatically in recent years and fully demonstrated China's weaknesses in the realm of cybersecurity.

First, although China has made due progress in its information and communication technologies (ICTs), as a late comer to this field, it still lags far behind other developed countries in many areas.

It would take a rather long time for China to narrow its technological gap with that of the advanced countries. In particular, numerous core cyber technologies are in the hands of Western countries, who enjoy a formidable technical edge and are at the upper stream of producing computer chips and web devices, while China is at the downstream of the supply chain, putting it in a disadvantageous position. The imbalances in the development of cyber capabilities between different regions and between urban and rural areas just make the situation even worse. Accordingly, China is in a state of cyber insecurity, with the recent Snowden and Prism event being a case in point. In the near future, this would be a fundamental challenge for China to safeguard its cybersecurity.

Second, although China has the largest number of netizens in the world, many of them are just green hands in accessing ICTs, often without any awareness or sense of cybersecurity.

Even the more educated people have little knowledge about cybersecurity, let alone the vast majority of the

common people. Upgrading software or patching security flaws might be easy, but people have to be alerted and told first of all and then educated on cyber (in)security. Briefly, a lack of cybersecurity awareness poses a direct threat herein.

Third, China is also faced with international peer pressures in cybersecurity.

Over recent years, numerous countries have strengthened their cybersecurity measures, *inter alia*, by building cyber armies. In particular, the U.S. established its Cyber Command in 2009 with a view to enhancing its offensive cyber capabilities. Many other countries are also busy with building their cyber armies, developing cyber weapons, conducting cyber exercises, and making ambitious cybersecurity policies. Although these moves are said to be defensive, many are of the nature of building offensive cyber capabilities, which could pose a serious threat to other countries, China included. These days, more and more people are also talking about the cyber arms race, which is surely an ominous trend that should be curbed and resisted.

Fourth, China is suffering from various cyber-attacks in the real world as well as in cyberspace.

China's Internet security watchdog CNCERT released a report covering 2013 on March 28, 2014. The report says that cyber-attacks from overseas on China's Internet are on the rise, while backdoor threats, phishing and trojans or botnets constitute three main forms of attack. In 2013, 31,000 overseas mainframes controlled 61,000 websites on the Chinese mainland through backdoor programs. Despite an annual decrease of 4.3 percent in the number of mainframes involved, the number of affected websites was up 62.1 percent compared to the previous year. Some 15,349 websites, about a quarter of the total, were attacked by 6,215 mainframes located in the United States. Moreover, 90.2 percent of phishing websites targeting Chinese users

were running on foreign servers. A total of 3,823 overseas IPs lured Chinese users to 29,966 fake websites to obtain passwords and other personal information, up 54.3 percent and 27.8 percent year on year respectively. U.S.-based servers hosted 12,573 fake phishing websites. In addition, 29,000 overseas servers controlled 10.9 million mainframes on the Chinese mainland via trojans or botnet. Servers originating from the United States hijacked 41.1 percent of all the mainframes, followed by those from Portugal and the Republic of Korea. The report suggests China map out a state-level strategy and devise more regulations to enhance cybersecurity.

Moreover , according to the reports by *Der Spiegel* and the *New York Times* based on the materials leaked by former NSA (National Security Agency of the United States) contractor Edward Snowden, the NSA conducted surveillance against the Chinese Huawei company, former Chinese top leaders, thus posing a severe threat to China's cybersecurity. So, in technical and real terms, China is faced with a severe cybersecurity situation.

1.6.4. *Means for strategic goals*

As for the policy measures, several aspects deserve our attention here.

First, China should have a deeper understanding and conduct more research on cybersecurity, including its technical, policy, strategic, economic, political, social, military, legal and international aspects. In particular, China should raise its awareness on cyber threats and cybersecurity.

Second, China should build its technical capabilities and narrow digital gaps. Just as mentioned above, disadvantages in cyber capabilities constitute a fundamental challenge to

China's cybersecurity. Therefore, in the future, China still needs to upgrade its cyber capabilities, including improving its cyber infrastructure, thus gradually narrowing its digital gaps with the more advanced countries.

Moreover, China will also provide due help and aid to other developing countries in their Internet development so as to realize its goal of advancing common and equitable development of cyberspace for all countries, thus infusing (injecting) impetus for their cyber capability-building to safeguard their cybersecurity.

For example, in 2009 China signed with ASEAN and Shanghai Cooperation Organization (SCO) respectively the China-ASEAN Coordination Framework for Network and Information Security Emergency Responses and the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, both of which have greatly promoted regional cooperation on cybersecurity issues. Of course, every country should join this international cooperation process in the future.

Third, China needs to enhance intra-governmental coordination. In other words, China needs to enhance the coordination between different governmental departments and strengthen its institutional capability building in cyber field.

Just like other countries, there are different departments in charge of different dimensions of cyber issues. The Ministry of Industry and Information Technology (MIIT) is more of a technical orientation, the Ministry of Public Security (MPS) has a focus on combating cybercrimes, while the Ministry of Foreign Affairs (MFA) is responsible for those diplomatic activities connected with cybersecurity. Other governmental departments also have their own function to perform.

It is natural that these different departments have different views, visions and perspectives on cybersecurity. Therefore, to harvest the potential benefits to the largest degree on the one hand and to maintain and safeguard cybersecurity on the other hand, effective coordination among these departments is not only needed but also a must in their daily work. Now, the good news is that the Central Leading Group on Cybersecurity and Informationization has been established, and is expected to play a central, leading and coordinative role in all aspects of cybersecurity in China.

Last but least, China should further promote international and bilateral cyber cooperation, which is an inalienable dimension of cybersecurity. Besides what has been said in the previous section, the following also deserves our attention.

In recent years, the international community has been calling for rules for cyberspace to be made, in the process of which all countries are indispensable. In particular, the United States and the West have been very active in an attempt to formulate cyber rules. In September 2012, Mr. Harold Hongju Koh, legal advisor of the U.S. Department of State, presented the U.S. views on international law in cyberspace during a USCYBERCOM Inter-Agency Legal Conference. In the same month, NATO also tabled its Tallinn Manual[28], exploring the applicability of the International Humanitarian Law (IHL) in cyberspace. Before that, in September 2011, China, Russia, Tajikistan and Uzbekistan also proposed a draft "International Code of Conduct on Information Security" at the UN General Assembly.

28 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 Cyberdefence Center of Excellence*, Cambridge University Press, 2013.

Although China hoped the international community could have in-depth discussions within the framework of the UN Group of Governmental Experts on the Issue of Information Security and reach agreement at an early date, the draft proposal was "largely dismissed by Washington and its Western allies". However, just as Mr. Amitai Etzioni, a senior advisor to the Carter White House, said, "if one did not know which nations submitted this proposal, one could easily assume that 95 percent of the draft code was composed by Western nations led by the United States".[29] Therefore, China, a member of the developing countries, and the United States, a representative of the developed countries, have so many common interests in cyberspace that it is a must to initiate talks on the draft proposal, during which more common grounds could be found and deeper mutual trust be built.

As the Stuxnet worm against the Iranian nuclear facilities demonstrates, cyber tools and weapons could lead to catastrophic scenarios. Therefore, the international community could negotiate an agreement to constrain the research, development and use of cyber tools and weapons, drawing on the experiences of the conventions on nuclear, chemical and biological weapons. Though cyber tools and weapons are unique and hard to verify, limiting cyber weapons could become a new direction for international cyber negotiations. The international community could also step in this thorny field, contributing to international cyber peace and security.

Accordingly, China thinks that cyberspace should be used for peaceful purposes and every country and man should enjoy the enormous benefits brought about by the development of the Internet. The lessons and tragic

29 Amitai Etzioni, "China Might Negotiate Cybersecurity", *The National Interest*, March 14, 2013, http://nationalinterest.org/commentary/china-might-negotiate-cybersecurity-8222.

consequences of the two world wars should not be discarded, and therefore, the trend towards militarization and weaponization of cyberspace should be strongly resisted, given the great potential damage it could incur.

Since cyberspace is not an isolated realm immune from the influence of relations in other fields, e.g. political and economic relations, we often have to view their cyber relations from a perspective of overall bilateral or international relations. To safeguard the peace and stability of cyberspace, efforts to maintain good state-to-state relations in other fields are also needed. Although the West, particularly the United States, is keen on accusing China of the cyber-attacks it suffers, today they are in fact faced with common cybersecurity threats/interests.

Cyberspace is a new domain for security studies with many questions to be figured out. Despite the fact that China is one of the major victims of cyber-attacks, just as in other domains in international relations, China has once again become the default target for accusation when the West, particularly the U.S., tries to release its complaints and find a scapegoat for the cyber-attacks from which it suffers.

Though China's positions are crystal clear, the West seems to have formed a bad habit of accusing China whenever something unpleasant occurs. On the contrary, China has always embraced a modest, low-profile and even humble approach to foreign affairs, which is different from the bold, assertive, and even aggressive one of some other countries. China also advocates and practices an active defense policy, which is defensive rather than offensive in nature. This also applies to the new domain of cyberspace.

Given the difficulty in cyber-attack attribution, *inter alia*, the transnational and anonymous nature of cyber threats, it is neither professional nor responsible to make groundless

accusations without hard evidence and is also not conducive to solving relevant problems. That is why China seldom publicizes or blame others for the cyber-attacks it suffers, thereby a Chinese way of performing cybersecurity is in the making.

1.7. Conclusion

China is a latecomer to the cyber field, but it has achieved enormous progress in the development of the Internet. It sees Internet development as part of its great cause of reform, opening up and modernization. It has put forward and implemented active and vigorous policies towards the Internet.

China adheres to the principle of scientific and effective Internet administration by law. It has formulated an effective and overall system of Internet administration, which is a combination of laws and regulations, administrative supervision, self-regulation, technical protection, public supervision and social education.

China has promoted international cooperation on cyber issues in an active manner. It has conducted various strategic and security dialogues and consultations on cybersecurity with numerous countries, carried out legal cooperation on fighting against cybercrimes, engaged in technical cooperation in addressing cyber incidents on a daily basis, and so on.

China has not yet produced a cybersecurity strategy as of April 2014, but the international cybersecurity situation will make China think more about it. The establishment of the Central Leading Group on Cybersecurity and Informationization will add a new impetus to this process.

Given the interconnected nature of cyberspace, noone could go it alone. Therefore, to tackle increasing cybersecurity hazards, international cooperation is needed. Specifically, enhanced technical cooperation among experts will yield twice the result with half the effort; on the governmental level, all countries should reinforce mutual trust and share best practices and experiences; on the operational level, various organizations also need to work with each other as cyber threats are always transnational ones. In a word, new steps and thinking are needed to advance cybersecurity and to build a peaceful, secure, open and cooperative cyberspace. This is what China advocates and practices.