CHAIRE DE CYBERDÉFENSE ET CYBERSÉCURITÉ
FONDATION SAINT-CYR THALES SOGETI

China’s Internet Development and Cybersecurity policies and practices

Xu Longdi (CIIS, Beijing, China)

Conference: “China’s Cybersecurity and Cyberdefense policies and strategies” - Paris, 1 July 2013

July 2013, Article n°VI.1.b

After land, sea, air and outer space, cyberspace has been dubbed as the 5th domain for human activities. Today, cyber security is closely connected with political, economic and security interests of States. Moreover, given the borderless and transnational nature of cyberspace, it has also has become a new frontier for global governance. China attaches great importance to Internet development and has made enormous progress. However, Internet is a double-edged sword, and as a late comer in this field, China also 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.

Ⅰ. Internet development in China

China came relatively late to the Internet, but the Internet has witnessed a rapid and sound development since its inception in China. During the mid-and-late 1980s, China’s researchers had tried actively to use the Internet. On such occasions as the 1992 and 1993 International World Wide Web Conferences, the experts from the Chinese computer community had asked more than once to be connected to the World Wide Web, and gained the understanding and support of their international peers. During the China-U.S. Joint Conference on Science and Technology Cooperation held in Washington in April 1994, the Chinese delegates and the U.S. National Science Foundation ultimately came to an agreement on China’s access to the World Wide Web. On 20 April 1994, a 64k special line was initiated, and the CAINONET for Education and Scientific Research in Zhongguancun, Beijing was connected to the World Wide Web, thus realizing its full-function connectivity with the World Wide Web and marking the official access of China to the World Wide Web[1].

After years of development, as of the end of December 2012, there has been 564 million netizens in China, with an increase of 50.9 million netizens in 2012, while the Internet Penetration is 42.1%, an increase of 3.8% compared with that of 2011. In the meantime, the number of mobile-phone netizens also experienced a rapid growth, being 420 million in 2012 with an annual growth rate of 18.1%. Now, the number of Chinese netizens is on a historical high level, with its growth rate and penetration reaching a period of relative stable development. Moreover, the scale of the netizens accessing to the Internet in Internet cafe and school computer room witnessed a sharper drop, with the former being 5.5% while the latter being 3%. On the contrary, the percentage of household Internet-accessing

[1] State Council Information Office, *White Book 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.

netizens (accessing the Internet at home) continued to be on the rise, being 91.7%, with an increase of 3.4%. Among others, the main reasons for this phenomenon are the increase of personal web devices, as well as improvement in the conditions of Internet access. By the end of December 2012, there have been 309 million micro-blog users, an increase of 58.73 million compared with that as of the end of 2011, while 54.7% of the Chinese netizens are micro-blog users. In particular, the scale of the mobile-phone micro-blog users is as high as 202 million, accounting for 65.6% or near 2/3 of all micro-blog users[2].

E-commerce, especially online shopping and group purchase (buying), has also experienced a high rate of growth, with mobile-phone-end commercial applications expanding rapidly. As of December 2012, the number of online-shopping users has reached to 242 million, an increase of 48.07 million compared with that of 2011, with a growth rate of 24.8%. While the growth rate of netizens has gradually slowed down, online shopping has maintained a momentum of rapid growth. Group purchase data demonstrates that there are 83.27 million group buying users (whose usage rate has increased from 2.2% to 14.8%), with a growth rate of 28.8% in 2012.

While network marketing is gaining more attention and the netizens are changing their consumption concepts, a lot of businesses have also begun to break their mono-business model, adding Internet channels to their traditional ones to seek new growth points for their sales. Briefly, traditional businesses are deepening their uses of Internet channels, while traditional and Internet channels are also being increasingly integrated.

While the Internet economy develops quickly, its application in e-commerce by the mobile-phone end-users also expands swiftly. Compared with 2011, online shopping through mobile-phones by the netizens increased 6.6% in 2012, and the number of users is 2.36 times as many as that in 2011. Moreover, the percentage of the netizens using group purchase, online payment and online banking through mobile-phone has also increased to some extent, with their net number increasing more than 80%.

Ⅱ. 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 informatization.

First, 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 Informatization, 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 Informatization Program during the 9th Five-year Plan and Goals in 2010, which brought Internet into the construction program of national information infrastructure and proposed to boost the process of national economic informatization by striving to develop Internet industry. Five years later in 2002, China promulgated its Specialized Informatization Planning Program during the 10th Five-year Plan on National Economic and Social Development, which set out the priorities for China's informatization 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 informatization and promote informatization through industrialization, thus opening a new way of industrialization. In November 2005, China laid down its

[2] China Internet Network Information Center (CNNIC), *The 31st Statistical Report on the Status of China's Internet Development*, 15 January 2013; 中国互联网络信息中心：《第31次中国互联网络发展状况统计报告》，2013年1月。http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/P020130122600399530412.pdf.

National Informatization Development Strategy 2006-2020, which was a long-term or strategic document on informatization development, further clarified the priorities for China's Internet development, and proposed to advance national economic informatization centered on readjusting economic structure and transforming 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 informatization and 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 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.

Second, in addition to lending full policy support to Internet development, China also invests heavily in building Internet infrastructures. From 1997 to 2009, China invested 4300 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.

Third, the construction and improvement of Internet infrastructure facilitates the spread and application of Internet. As of the end of 2009, there had been 3.23 million websites within China, 2152 times as many as that in 1997, and about 2300 million IPv4 addresses, ranking the second in the world, according to the *White Book*. By the end of 2012, China had altogether 13.41 million domain names, among which 7.51 million are those ends with .CN, accounting for 56.o%, and 280,000 domain names ends with .中国, according to the *31st Statistical Report*. After a fall in the number of websites (i.e. the number of websites within China possessed by domain registers, including both those of accessing from within and without) during the past several years, as of the end of 2012, the figure rose again to 2.68 million.

Fourth, 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.

Fifth, China practices a policy of managing cyber affairs in line with law, adhering to the principles of scientific and effective management in its Internet governance. It also endeavors to improve its Internet management 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 management, including the NPC Standing Committee Decision on Safeguarding Internet Security, the PRC Electronic Signature Law, the PRC Telecommunication Regulations, Internet Information Service Management Methods, the PRC Computer Information System Protection Regulations, and so on. To be sure, China will continuously improve its Internet governance through practices. China also advocates the free and secure flow Internet information, which are not only the two sides of the same coins, but also constitute an indispensable and interdependent whole. It sticks to combat cyber crimes 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.

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 informatization, 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, Urban netizens account for 72.2% of all Chinese netizens, while that of the rural netizens was only 27.8%. 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 continue to promote Internet development and spread, thus making more people benefit from it.

Ⅲ. Challenges facing China's cybersecurity

While China has gain great progress in developing its Internet, as with others, it also faces various security challenges in cyberspace. As a matter of 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 of all, 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 a lot of 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, making 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 to ICTs, often without any awareness or sense of cybersecurity. Even those most educated people have little knowledge about cybersecurity, let alone a vast majority of common people. Upgrading a software or patching security flaws might be easy, but the people have to be alerted and told at first and then educated on cyber (in)security. Briefly, lack of cybersecurity awareness poses a direct threat herein.

Third, China is also faced with international peer pressures in cybersecurity. During the past 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 cyber armies, developing cyber weapons, conducting cyber exercises, and making ambitious cybersecurity policies. Although these moves are said to be defensive, many are in nature to build offensive cyber capabilities, which could pose serious threat to other countries, China included. These days, more and more people are also talking about cyber arms race, which is surely an ominous trend that should be curbed.

Fourth, China is suffering from various cyber attacks in the real world as well as in cyberspace. For example, last year, 52,324 websites in China were installed backdoor programs, among which 3,016 websites are governmental ones, an average increase per month of 213.7% and 93.1% respectively compared with that of 2011. China also suffered from serious advanced persistent threats (APT) in 2012, with at least 41,000 host computers within China, covering numerous governmental organs, and key information and high-tech institutions, being infected with such APT-type Trojan programs as Flame and Gauss, whose control servers are mostly located outside China. Moreover, more than 14,197,000 host computers in China were remotely controlled by approximately 73,000 foreign Trojan or botnet control servers in 2012, an increase of 56.9% and 59.6% respectively compared with that of 2011, among which 10,512,000 host computers within China were controlled by 12,891 control servers (17.6% of the total foreign control servers) located in the United States, ranking first in both the number of control servers and the number of host computers being controlled within China. So, in technical and real terms, China is faced with a severe cyber security situation[3].

As has been repeated by the Chinese leaders, including Premier Li Keqiang, State Councilor Yang Jiechi, and the spokesmen from the Ministry of Foreign Affairs and the Ministry of Defense, China is firmly opposed to hacking and the Chinese law prohibits any hacking behavior compromising Internet security. China also advocates and practices an active defense policy, which is defensive rather than offensive in nature and also applies to the new domain of cyberspace.

Ⅳ. What to do next: Chinese way of doing cybersecurity

Cyberspace is a new domain for security studies with many questions to be figured out. Despite of 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 it gets. 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 the United States.

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 doing cybersecurity is in the making.

First, further promote international and bilateral cyber cooperation. As a matter of fact, China actively promotes the establishment of bilateral dialogue and exchange mechanisms in this field. In an interdependent world, any country could not go it alone. In an interconnected cyber world, there is no absolute security for any state. 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. For instance, in their Strategic Security Dialogue under the framework of China-U.S. Strategic and Economic Dialogue (SED), the two sides have touched upon cyber security issues. The Internet Society of China and the U.S. think tank EastWest Institute also conducted a joint research and released a report on “Fighting Spam to Build Trust” in June 2011. All these are good signs and could constitute a starting point for future cooperation with a view to building a peaceful and secure cyberspace[4].

In addition, China has hosted China-U.S. Internet Forum (6 times) and China-UK Internet Roundtable (4 times) with the U.S. and the UK respectively since 2007. China also holds cybersecurity dialogues

[3] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cyber Security 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.

[4] "Fighting Spam to Build Trust", EastWest Institute and Internet Society of China, June 2011

and consultations with France, Germany, South Korea and other countries in recent years. In the field of combating cybercrime, Chinese public security organs have also participated in such international cooperation as the Asia and South Pacific Working Party under the Interpol working parties on Information Technology (IT) Crime and China-U.S. Joint Liaison Group on Law Enforcement, etc. All these are sign of China being open and practical to international cybersecurity dialogue and cooperation.

As one of the main channels for international cooperation in China’s computer emergency response system, the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) also engages in practical and technical cooperation with other countries in addressing cross-border cybersecurity incidents. For instance, it carries out an "international cooperation partnership program" and has established contact mechanisms with 91 organizations from 52 states by the end of 2012. It has officially signed MOUs on cybersecurity cooperation or reached agreements with 12 of the 91 organizations, and has gradually improved and enhanced the collaborative mechanisms on addressing cross-border cybersecurity incidents. 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 the ones against foreign banks and companies, such as the Bank of America (BOA), the National Australia Bank and PayPal. In October 2012, CNCERT got a complaint (request) from the USCERT, which claimed that some of the host computers located in China were controlled by malwares and participated in DDoS attacks against certain US bank and company, 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 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[5].

Second, the international community is calling for making rules for cyberspace, in the process of which all countries are indispensable. In recent years, the United States and the West have been very active in an attempt to formulate cyber rules. Last September, 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, 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[6]. 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”. 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[7].

Third, as the Stuxnet worm against the Iranian nuclear facilities demonstrates, cyber tools and weapons could lead to catastrophic scenarios. So, the international community could negotiate an

[5] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cyber Security 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.

[6] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare - Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press, 2013.

[7] Amitai Etzioni, “China Might Negotiate Cybersecurity”, *The National Interest*, March 14, 2013, http://nationalinterest.org/commentary/china-might-negotiate-cybersecurity-8222

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 the cyberspace should be used for peaceful purposes and every country and man should enjoy the enormous benefits brought about by the development of Internet. The lessons and tragic consequences of the two World Wars should not be discarded, and therefore, the trend of militarization and weaponization of the cyberspace should be strongly resisted, given the great potential damage it could incur.

Fourth, building technical capabilities and narrowing digital gaps. Just as I mentioned above, disadvantages in cyber capabilities constitute a fundamental challenge to China's cybersecurity. So, in the near future, China still needs to upgrade its cyber capabilities, including its cyber infrastructure, thus gradually narrowing its digital gaps with other advanced countries. Moreover, China will also provide 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, China signed in 2009 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, which greatly promote regional cooperation on cybersecurity issues. Of course, every country should join this process.

Last but not least in importance, 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. In the meanwhile, cyberspace is not an isolated realm immune from the influence of China-West (U.S.) relations in other fields. Therefore, 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.

Conclusion

In sum, to build a peaceful, secure, open and cooperative cyberspace, and to tackle increasing cybersecurity hazards, a multi-level, multi-channel, and multi-form of international cooperation are 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 classical cases and experiences. On the operational level, various organizations also need to work with each other as many cybercrimes are transnational ones. In a word, new steps and thinking are always needed to advance rather than reverse cybersecurity, which needs efforts from all sides.

Chaire Cyber-Défense et Cyber-sécurité

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
La chaire remercie ses partenaires

ARMÉE DE TERRE

CENTRE DE RECHERCHE
DES ÉCOLES DE
SAINT-CYR COËTQUIDAN

FONDATION SAINT-CYR

SOGETI

THALES