Sociology Study, November 2015, Vol. 5, No. 11, 825-831
doi: 10.17265/2159-5526/2015.11.001

National Cybersecurity Strategy of the U.S. and Its Constructive Implication for China

Bowei Shi[a]

Abstract

Deteriorating continuously, cybersecurity issue has become the focal point of global attention and the grave concern from countries of the world since around 2010. The United States, a country of most developed internet technology, is also the most serious victimized country subjected to cyber attacks. After more than 10 years of tremendous funding and energy investment, the United States, at present stage, has built a relatively impeccable, government-led system of cybersecurity strategy. This strategic system is characterized by a full-fledged combination of offensive and defensive capabilities which takes full advantage of America's technological superiority, and the primary purpose of this system is forming strategic deterrence. This paper is designed to provide an interpretation of the specific components and nature of this strategy and hopes to reveal the possible enlightenment on how to manage cybersecurity discrepancy between China and America and its constructive implication to China's construction of cybersecurity strategy.

Keywords

The United States, cybersecurity strategy, China, constructive implication

Currently, internet technology, being acknowledged as "the nerve center" of modern human life, has permeated nearly all sorts of domains related to national, corporate, and individual interests, including business, financial area, manufacturing industry and critical infrastructure construction field, etc. Nevertheless, the cybersecurity issues—different degrees of damage to the integrity, confidentiality, availability, controllability of information loaded in cyberspace—have been severely confronting the world with its devastating effect. The amount of cybersecurity incidents and the subsequent economic losses resulted herein have increased dramatically every year since the beginning of new millennium. According to incomplete statistics, the direct financial losses have deteriorated appallingly from 13 billion dollars in 2001 to 445 billion dollars in 2014. Personal information interception and intellectual property infringement are the most prominent and urgent to be solved problems testing present cybersecurity situation. In addition, cyber attacks and cyber espionage aimed at military field and critical infrastructures construction, which are vital to national security and lifelines of the national economy respectively, have also been rampant and drawn grave concern among nations and international community.

Three main reasons can be accountable to the grim reality: The first is the inherent defects of the internet technology resulting from its permanently relative

[a]Sichuan International Studies University, China

Correspondent Author:
Bowei Shi, Graduate School, Sichuan International Studies University, No. 33 Zhuangzhi Road, Shapingba District, Chongqing, China, 400031
E-mail: 1164909724@qq.com

immaturity; the second is that the research and development of network defensive technique and the formulation of defensive policy always lag behind the rapid progress and enrichment of cyber attack methods; last but not least, due to the intrinsic "anarchy" of cyberspace and the irreconcilability of the interests possessed by state actors or non-state actors, international community, heretofore, have not established an efficient co-administration mechanism concerning about cybersecurity, and the legislation of relevant domestic laws and international laws is also proceeded awkwardly. All the three reasons provide the act of cyber attacks with a vacuum free from regulations.

The Unites States government serves as the core leadership in developing its national cybersecurity strategy. The George W. Bush administration issued the national strategy to secure cyberspace and related policy directives as early as 2003 and by the end of Bush's presidency, the rudiment of the national cybersecurity strategy has been formed. After years of tremendous funding and energy investment, the United States, at present stage, has built a relatively impeccable, highly effective, government-led system of cybersecurity strategy which attaches great importance to the role of private information enterprises and possesses consummate project of cultivation and reserve of talents. This strategic system is characterized by a full-fledged combination of offensive and defensive capabilities which takes advantage of America's technological superiority and aims at forming strategic deterrence.

The paper will focus on the specific components of this strategy and their possibly constructive implication for China.

NATIONAL CYBERSECURITY STRATEGY OF THE U.S.

The Background of This Strategy

Since cyberspace depends completely on technology, the mastery of core technology means, for the cyberattacking actors, the mastery of core attacking technology. The immanent "vulnerability" of internet technology caused by the gaps between theory and practice and the backwardness of cyber defensive tactics make those nations who have excessive reliance on internet to perform various activities, especially economic and political activities, become vulnerable to antagonistic states and terrorist actors. In his book *Cyberdeterrence and Cyberwar*, Martin C. Libicki (2009), the senior management scientist at RAND Corporation, said: "As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk". By this token, the United States, who has developed the internet technology at the furthest level among the world, is the most vulnerable to attacks by hostile forces. And the United States indeed is the worst-hit country in terms of frequency, degree of cyber attacks and financial losses caused by cyber attacks. In the early period of the Obama administration, all circles of American society were convinced that cyberattacks had replaced terrorism as the principle threat to its economic and military security. The three annual reports (2013, 2014, 2015) Worldwide Threat Assessment of the US Intelligence Community rank "cyber", without exception, as the number-one threat among their list of "Global Threats". In its 2013 Worldwide Threat Assessment of the US Intelligence Community, James R. Clapper, the director of National Intelligence, said:

> We are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of—and interaction with—the world are becoming more intertwined with digital technologies and the Internet. In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks... The growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behavior... In response to the trends and events that

> happen in cyberspace, the choices we and other actors make in coming years will shape cyberspace for decades to come, with potentially profound implications for US economic and national security. (Clapper 2013: 1)

From this passage, it can be seen that the United States has been fully aware of the infiltrative role played by internet technology in every field and admitted that, compared with the application of internet techniques, its cognizance and reflection of cybersecurity issues and their possible implications fall behind relatively. The American government also recognized that the strategy to be taken would decide the future situation of cyberspace. For the United States who has achieved the global hegemony almost a century ago and possesses absolute supremacy of internet technology over other nations, the strategy adopted is definitely inclined to strive for the effective integration of attacking and defensive tactics and even to "strike first to gain initiative", rather than to treat cyber threats with pessimistic indifference or to defend passively.

Specific Components of This Strategy

This strategic project consists of five principle elements: joint management and control by several specialized governmental agencies, domestic legislation on cybersecurity, dedicated collaboration of government agencies and private internet corporations, research and development of cutting-edge technology and talents cultivation, and international cooperation.

(1) Establishing relevant government organizations. The US government has set up several agencies specializing in guaranteeing information security to institutionalize the whole network cause. The national security strategy of the Bush administration and the related policies promoted the emergence of Department of Homeland Security which was assigned multiple leadership roles and responsibilities in this area. The United States Cyber Command, which undertook the integrated planning of defense, capability building, and emergency processing when facing unexpected cyberattaks, was founded by the Obama administration in 2009; the Department of Defense set up a Chief Information Officer; some veteran offices such as National Security Agency and United States Strategic Command appointed cybersecurity officers; the Federal Bureau of Investigation also set up an office to investigate cyber crime. In addition, the American government consistently attached great importance to intelligence sharing to avoid inefficient communication among these agencies. In the 2013 National Security Strategy report, the US government admitted that "Non-cooperative organizational structure created failures to share information between the various intelligence agencies prior to the September 11th attacks", promised that "The United States cannot suffer from similar failures again", and appealed for that "The United States must develop standards for sharing cyber security information among government and military branches" (Obama 2013: 5). Owing to remarkable coordination, these special intelligence agencies, at present, own mature criteria and consensuses on information sharing and responsibility assignment, protecting intelligence security efficiently in America;

(2) The legislation of domestic laws. Some information incidents have already aroused legislative bodies' vigilance and urged them to enact relevant laws in that area, since computer technology was applied with medium scale by government and private giant corporations in 1980s. Several specific statutes were enacted at that time, among them the most notable are The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, The Electronic Communications Privacy Act (ECPA) of 1986, The Computer Security Act of 1987, etc. (Fischer 2013: 52-61). These laid a firm foundation for the subsequent legislation of cybersecurity. The 9/11 terrorist attack was the turning point, the legislative process in that area quickened since then. The congress passed six important statutes in the year of 2002 alone, including Homeland Security Act

(HSA) of 2002, Cyber Security Research and Development Act 2002, and Federal Information Security Management Act (FISMA) of 2002. The House of Representatives and Senate also established Permanent Select Committee on Intelligence and Committee on Homeland Security and Governmental Affairs respectively to take charge of legislating laws on cybersecurity. After Snowden's revelation of classified surveillance programs on the part of the United States government, the congress promulgated Cybersecurity Enhancement Act of 2014, National Cybersecurity Protection Act of 2014, and Cybersecurity Workforce Assessment Act in succession to defuse the public resentment and renovate its contaminated international image. Besides, American specialists on cybersecurity have been proposing proactively revisions to those out-dated "antique" bills and trying to make them adopted by the congress. At present, the United States' legislative work on cybersecurity was relatively elaborate and mature as compared with other countries (It has enacted more than 50 relevant acts), those laws are functioning effectively on the cyber defense, deterrence, and *ex post facto* attribution;

(3) The collaboration between government and private internet corporations. The reason why the computer technology in America has obtained supremacy over all the globe is because there exists a plenty of distinguished private internet companies, such as Google, Microsoft, Yahoo, Facebook, etc. The effective implementation of national cybersecrity strategy, to a large extent, depends on the technology provided by these giants to be utilized by the government as powerful "defense shield" and "attacking sword". The American government has profoundly recognized the significance of this kind of cooperation. Michael S. Rogers (2014), Commander of U.S. Cyber Command and director of National Security Agency (NSA), claimed that, "The challenges (in cyberspace) are so broad... It is going to take a true partnership between the private sector, the government and academia to address (them)". The United States government is committed to providing collaborative avenues through which private cybersecurity firms can share sensitive information with the government in order to prevent increasingly worsening cyber attacks;

(4) Facilitating the research and development of advanced network technology and computer professionals training. The United States spares no efforts in facilitating the research and development of advanced network technology and computer professionals training. The multitudinous prestigious academic institutions and internet enterprises could provide technical support for the achievement of both defensive and offensive capabilities. Now that cybersecurity issue has become the focal point of global attention, the occupation of cybersecurity engineers has also become more desirable and decent than ever before, attracting many high-tech talents engaging themselves into this area. Additionally, the sufficiently developed high-education system of the Unites States could contribute top human resources for the cause of cybersecurity;

(5) Seeking cooperation among international community. It has been fully acknowledged by the US government that since the cyberspace belongs to "Global Commons" (public realm), curbing cyber crimes and defensing cyber attacks need cooperation among international community. The United States' strategy of international cyber cooperation has no special restriction on partner countries' attributes. On the one hand, the United States positively conducts all-round collaboration with its North Atlantic Treaty Organization (NATO) allies on joint cultivation of qualified personnel, establishment of bilateral or multilateral cyber defensive mechanism, practice exercise of cyberattacks, and the like. For instance, the Estonia-initiated NATO Cooperative Cyber Defence Center of Excellence and NATO Cyber Defence Management Authority were founded at Tallinn in May 2008 and Brussels in the end of 2008

respectively, which have deepened their collaboration in that area. Similarly, the United States has also developed limited cooperation with countries it condemned as cyberattack actors, such as China, Russia, etc. For example, pushed by Chinese President Xi Jinping's recent state visit to the United States, both sides reached an important consensus on joint striking cyber crime and commitment of holding regular cybersecurity dialogues.

The Nature and Prospect of This Strategy

The report of National Security Strategy 2013 pertaining to cybersecurity proclaimed that, "We must prepare for the future of defense through the development of both defensive and offensive cyber capabilities" (Obama 2013: 5). By this token, this national cybersecurity strategy, since its inception, has intended to "forge" a cyber force integrating destructive attacking power with impregnable defensive power, thus creating a strategic deterrent effect among the globe. Every nation should be wary of the intense "aggressive tendency" revealed in this strategic system.

Since the Snowden incident, the United States has made partial adjustment to its cybersecurity policy to cope with great pressure from international public opinions. For instance, it handed over the right of supervision of Internet Corporation for Assigned Names and Number (ICANN) who manages 13 top-level root name severs and accelerated legislation process on cybersecurity. Nevertheless, these trivial adjustments will not change the general direction of this strategy.

THE CONSTRUCTIVE IMPLICATION FOR CHINA

Conflicts and Cooperation on Cybersecurity Between the U.S. and China

In one of its April (2015) report titled "A New U.S. Grand Strategy Toward China", the Council on Foreign Relations asserted and suggested that, "The United States needs to fundamentally change its grand strategy toward China" (Blackwill, Kissinger, and Tellis 2015). This report typically reflects the mindset of American political circles toward China's rise and the conflicts between the established power and the emerging power are so deep-rooted that it cannot be reconciled effortlessly. The main discrepancy on cybersecurity between the two largest economies is that both sides "have serious differences on cyberattacks and the rules of cyberspace as well as how to ensure the security of the hardware and software of each country's information and communications infrastructure" (Innes-Ker et al. 2015). In its annual report Worldwide Threat Assessment of the US Intelligence Community, the United States always denounces China as the principal actor who launches cyber espionage and attack against America's network system. However, the U.S. and China should sensibly recognize that the cold war mentality of antagonizing one side with the other would bring nothing but harm to bilateral relation. Actually, both the U.S. and China share partial common interests in preventing escalation of cyber threats. The preliminary consensus of curbing cyber crimes reached by the two sides in September 2015 and the sincerity of being willing to convene further and frank dialogues opened the door to starting official cooperation on cybersecurity. Both the United States and China expressed the good wishes to develop collaboration on the basis of limited consensus and seek deeper mutual trust in such collaboration. As Secretary of State John Kerry (2015) put it, "It is not relationship yet built on pure trust; it's relationship built on a clarity to the things we choose and work on together and try to build trust". Yan Xuetong (2015), Director of Institute of Modern International Relations in Tsinghua University, also pointed out recently that "Mutual trust is not the precondition of cooperation, on the contrary, cooperation is the precondition of mutual trust". Thus, the author of this paper maintains that in the area of

cybersecurity, the United States and China should collaborate closely to eliminate mistrust instead of provoking confrontation to harm each other.

Its Constructive Suggestions for China's Cyber Capability

Although China should be on guard against the aggressive tendency revealed in America's national cyber strategy, it is more noteworthy that what we can learn by studying the successful achievements of this strategy to develop China's "hard power" and "soft power" in the construction of secure cyberspace. As China has not yet issued its own cybersecurity strategy, the organizational mechanism, consciousness of cyber legislation, cooperation model of government and private corporations, experience of training professionals and seasoned international collaboration in the America's strategy are well worth studying.

First, in building its internet hard power, China should speed up the overall planning of founding relevant government agencies and reinforce and update the existing organizations in both quantity and quality. The Office of the Central Leading Group for Cyberspace Affairs founded in February 2014 marks the establishing a comprehensive government agency which co-ordinates the big-picture of constructing cyber capability. But it must be admitted that the newly-founded agencies, such as Bureau of Cybersecurity Management of Ministry of Industry and Information Technology, Supervision Bureau of Public Information and Cybersecurity of Ministry of Public Security, and so on, still have a lot of deficiencies on function division, emergency mechanism, and action capability, which should be improved immediately by coordinative management from the Office of the Central Leading Group for Cyberspace Affairs. And, since the lack of core computer technology is the bottleneck constraining development of cyber capacity of China, "We must possess our own technology, transcendent technology... and construct outstanding infrastructure and foster well-qualified personnel in the cyber and informatization area to build a cyber-powerful country" (Xin 2014). The development of national brand of network technology and training of world-class professionals necessitate more investment from government on cyber education and cyber research.

Second, in building its internet soft power, China should beef up supervision over the internet to improve its much-maligned national image as major cyberattacking actor. In addition, although the first special statute Cybersecurity Law (Draft) has been introduced to the public for soliciting opinions from all sides on July 6, 2015, it puts great emphasis on maintenance of personal information: "It, however, didn't deal much with public security issues which has posed severe threats to the cyberspace's operational order" (Liu Deliang 2015). The present grave climate of cybersecurity desperately necessitate that the Standing Committee of the National People's Congress (NPC) should expedite the legislative process pertaining to cybersecurity to change fundamentally the situation of relevant laws' absence and unevenness in legal system.

Third, in the aspect of international laws, as Chen Xiaogong (2015), Deputy Commander of People's Liberation Army Air Force (PLAAF), has said, "Since cyberspace is a new domain in global management, international community has not established the corresponding new order and new principles; what works, in practice, in cyberspace is still 'the law of jungle', that is cyber capability decides cyber right". As a Permanent Member of the United Nations Security Council and a major power with international influence, China is supposed to, as a vibrant initiator, collaborate with the major countries and international organizations to establish global co-administration mechanisms of cybersecurity to curb the deterioration of cyber crime and cyber espionage and substitute "the law of jungle" with more fair international code of conduct, thus creating a national image of "responsible great power".

References

Bartley, R. 2015. *US, China Reach Cybersecurity Agreement, Commit to Regular Dialogue*. Retrieved (http://www.fiercegovernmentit.com/story/us-china-reach-cybersecurity-agreement-commit-regular-dialogue/2015-09-25).

Blackwill, R., H. Kissinger, and A. Tellis. 2015. *A New U.S. Grand Strategy Toward China*. Retrieved (http://www.cfr.org/china/new-us-grand-strategy-toward-china/p36435).

Chen, X. G. 2015. *A Speech on the 13th Forum of "The Oder of International Cybersecurity" of Institute of Modern International Relation, Tsinghua University*. Retrieved (http://www.imir.tsinghua.edu.cn/publish/iis/7246/2015/20151015104524124852434/20151015104524124852434_.html).

Clapper, J. 2013. "Worldwide Threat Assessment of the US Intelligence Community." A Report of Senate Select Committee on Intelligence by James R. Clapper, Director of National Intelligence. Retrieved (http://www.nctc.gov/docs/2013_03_12_SSCI_Worldwide_Threat_Assessment.pdf).

Fischer, E. 2013. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. Retrieved (http://fas.org/sgp/crs/natsec/R42114.pdf).

Innes-Ker, D., E. Economy, D. L. Shen, A. Segal, and O. H. Schell. 2015. *How to Improve U.S.-China Relations*. Retrieved (http://www.cfr.org/china/improve-us-china-relations/p37044).

Kerry, J. 2015. *A Video File of a Very Renowned Talk Show—Yang Lan Interview Transcription*. Retrieved (http://www.iqiyi.com/v_19rrknr0co.html?vfm=2008_aldbd).

Libicki, M. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Liu, D. L. 2015. *The Toxicity of Trojan Horse Virus Bear Resemblance With That Firearms*. Retrieved (http://www.iolaw.org.cn/showNews.aspx?id=45963).

Obama, B. 2013. *National Security Strategy 2013*. Retrieved (http://www.utexas.edu/lbj/sites/default/files/file/news/National%20Security%20Strategy%202013%20(Final%20Draft).pdf).

Rogers, M. 2014. *Cybersecurity Threats: The Way Forward*. Retrieved (http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy).

Xin, J. P. 2014. *Building a Cyber Superpower*. Retrieved (http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm).

Yan, X. T. 2015. *The Deficiency of Mutual Trust Should Be the Obstacle of Cooperation*. Retrieved (http://pit.ifeng.com/a/20151020/45746479_0.shtml).

Bio

Bowei Shi, BA, postgraduate majoring in American Study, Graduate School, Sichuan International Studies University, Chongqing, China; research fields: American history and foreign policy.