Development of the U.S. Cyber Security Strategy Legislation and the Enlightenment for China

Jia-hao YANG

Zhongnan University of Economics and Law, College of Criminal Justice, Wuhan, China

youngpaper@126.com

Keywords: Cyber security strategies, cyber security legislation, mastery of the cyber.

Abstract. Since 2011, the global arms race of cyber is intensifying. In order to realize the cyber deterrence and seek the strategic advantage, USA has issued some programmatic documents to promote the development of cyber security, including National Strategy for Trusted Identities in Cyberspace, International Strategy for Cyberspace, Action Strategy for Cyberspace, and National Strategy for Information Sharing and Safeguarding. From the Clinton administration to the Bush administration, and to the Obama administration, USA is gradually developing cyber security-related aspects of organization control, network technology and military capabilities, aiming at taking further control over the power of setting the security standards and rules of international Internet in a new round of "network warfare". This work analyzes the development and characteristics of American cyberspace security strategy legislation and provides some enlightenment for our country.

Introduction

The United States is one of the first that has applied information technology to military area, national economy and social life. It is also one of highest informatization degree and best network technology countries. America's network security is the most important thing among the world. Especially after 911, America lays more stress on the construction and legislation research of software and hardware system of network security. It has issued continuously various law and regulation to enhance network security. In order to prevent the attack and damage of international terrorism through network, America promotes international cooperation on network technology and legislation with developed countries such as European Union and Japan, and also obtains enormous result. We will tease apart America's principle strategic development history and recent strategic move of network security as well as sum up the characteristics of its network security strategy to give some enlightenment and precedent for the speeding up network security and informationtization construction of our country.

For a period of time in the past, although no convincing evidence America has claimed that China is carrying out operation of network spy and intrusion to America. But ironically, the Snowden Events reveals that America has always been invading Chinese network system. In June 2013, Snowden, the former employee of the U. S. intelligence service revealed, the U. S. National Security Agency has extensively invaded major telecommunication companies to acquire cell phone message and continuously attacked main network of TSinghua University. Network interconnection makes network security to be of common challenge all countries over the world. This global problem could be solved only based on mutual participation and cooperation. The two sides agreed in the Sino US Strategic and Economic Dialogue framework, set up Network Security Work Group. The first meeting was held in July 8, 2013. China and U. S. communicated each other on network relations between two countries, international rules of cyberspace and bilateral talk and cooperation. In this background, it seems to be particularly necessary to know about network security policy and legislation of the U.S.

Analysis of U. S. Cyber Security Legislation

After analyzing comprehensively the legislation of network security of America, the following aspects are worthy of our country.

© 2016. The authors - Published by Atlantis Press

Establishment and Development of Cyber Strategy Objective. U.S. Cyber security strategy has undergone the development process of nearly half a century from the generation of the Internet strategy of Linden Johnson Government in 1964 to the development of Cyber security strategy of the real sense in the period of Bill Clinton administration to the maturity of Cyber security strategy in the period of Barack Obama administration. At this period, positive interaction was realized between the change of Internet strategic thinking resulted from the growth and prosperity of Internet in America and the international and domestic security environment of America in different periods of time. The intensified dependence of American national security on information network and the change of situation of American Cyber security environment have promoted the generation, adjustment and intensification of Cyber security strategy. As Cyberspace has become an important source of the threat to American national security, the position of Cyber security strategy in American national security strategy rises. Meanwhile, the formulation and implementation of U.S. Cyber security strategy are not merely on the "security" level, the political intention under which is thought-provoking.

Taking the above strategic objective as the core guidance, U.S. Cyber security strategy is characterized by in-time formulation and keeping pace with times. Cyber security strategy came into being during Bill· Clinton administration (1997-2001), which was in the transition period of American Cyber development from growth period to prosperity period. The main documents of Cyber security strategy at that time mainly aimed to promote American Cyber economy and protect the security of infrastructure of key departments. Although it needs to be improved, it laid solid foundation for follow-up work of the next government. George Walker Bush Government was influenced much by "9 · 11" event, and its "anti-terrorist" thought was the guidance during the adjustment of Cyber security strategy. During the administration of Barack Obama, the international political effect of network media becomes increasingly important, and power struggle during the international mechanism establishment intensifies, which makes American government focus its Cyber security strategy on international level. At the beginning of the 21st century, the "three-stage-development" of U.S. Cyber security strategy from Bill Clinton Government to Barack Obama Government shows us the characteristics of inheritance and development of strategic formulation, "from resistance to attack" of its status, and "inside-out transition" of security cooperation.

Accomplishment of National Strategy of Cyber Security. U. S. Cyberspace strategy is that of jostling the commanding point and mastery of cyberspace of world cyberspace from technology, resource, information and jurisprudence. It has brought omni-directional and multilevel impact to the cyberspace security of our country. The expansionary strategic objective of U.S. Cyber security strategy demands for solid resource base in implementation, and excellent talent team, eminent technological superiority, strong economic strength, powerful military guarantee, and rich political resource are important for the smooth implementation of the strategy. In May 2010 after the United States Cyber Command was formally launched, and the "criss-cross" implementation system of U.S. Cyber security strategy was established, the implementation efficiency of the strategy has been greatly improved. At present, American government is seeking for the security and prosperity of its Cyberspace, and protecting the national interests such as view of value and dominancy standardized by the principles of "security capacity building", "supremacy of national interests", and "participation and dominance" by taking control, threatening, interference and cooperation as the mode and means of strategic implementation.

Policy of Training of High-quality Professionals of Cyber Security. The U.S. government and military have long been put a high value on the cultivation and training of Cyber security professionals. It has issued various corresponding policy alongside development of Cyber security. U.S. National Security Agency set up Academic Center of Information Security in 1995, and started National Internet Education and Training Plan. The U.S. government also launched Cyber Academic Plan and Cyber Security Research & Development Bill in 2002. The National Institute of Standards and Technology (NIST) published National Cyber Security Education Program in 2010. The American Department of Homeland Security offered five targets for construction of information security specialists. On the push of the polices, a multilevel and wide-range development system of Cyber

talents is being already basically formed. According research of Rand Corporation, private agency and public sector have already found the way to solve shortage of Cyber security talents. The enormous requirements of Cyber security talents could be basically satisfied based on current market mechanism. The U.S. government pays much attention to train well-educated talent of federal administration Cyber security and increases its size, and especially enhances the training of next generation's Cyber security talents. The Cyber security specialists keep frequent communication with those of private agencies.

Attaching Importance on Research of Cyber Security Technology. In 2002, U.S. government has issued Cyber Security Development and Research Act in which the National Science Foundation and National Institute of Standard and Technology were endowed with duty of Cyber security research. It pays attention to the exertion of colleges and social research agencies. Many universities have set up schools, research centers and majors related to information technology and Cyber security, for example, the Software Engineering Institute of Carnegie Mellon University, Cyber Security & Privacy Research Institute of Georgetown University, National Computer Security Association (NCSA), Technical Committee of Center for Strategic and International Studies (CSIS), the information revolution and international relations projects of Carnegie Institute for International Peace and etc.

Implication for Chinese Legislation of Cyber Security

Formulating Middle and Long-term Strategic Planning of National Cyber Security and Focusing on Top-level Law-making. The administration should establish the middle and long-term strategic planning of national Cyber security, especially construct and firm up the five system of national Cyber security, namely, certification system of Cyber security technical standards, self-discipline system for formulation of norms of Cyber security industry, access, use and protection system, supervision and enforcement system of cyber security infringement, law and regulation system of cyber security.

Mapping Out Over-all Planning of Legislation and Extending Research of Basic Legislation of Cyber Security. Cyber security legislation should lay stress on organic unify of national interest and concord principle. Information security should primarily be embodied in national interest, avoid repeated and distributed legislation, increase coordination of legislation as well as save from blindness, arbitrariness and competition. We should enhance research of legislation function, value orientation and fundamental pattern of cyber security, set up basic theory of cyber security law system, conduct over-all sorting and follow-up to international legislation experience system, sum up completely the path, flaw and development direction of domestic cyber security legislation, raise theory and legislation framework of system tree, bolster the scientificity, authority and foreseeability of cyber security legislation.

Insisting on Equal Protection of National Cyber Security and Individual Information. Equal protection of cyber security and citizen individual information must be treated as important principle of cyber security legislation. Some of the earlier legislation have unduly strengthened the government's cyber control and ignored protection of civil rights of related cyber space. Legislation of cyber security of mobile internet must emphasize on priority of national security, combination of government guide and self-discipline of industry system, protection of cyber liberty, maintenance of interest balance, protection of individual information and keeping public order of cyber. Meanwhile, we should insist on the solution of problem about equality of opportunity, regulation and institution that is protected by forgotten right. Thus mutual balance of individual information interest and efficient protection of national cyber security will be realized.

Establishing Ideal of Following Existing Legal System and Also Breaking Through It When Necessary. We should fully study the ideal of U.S.A, that is, that to impose system configuration of every agency by formulation of law and regulation may influence other better ways to solve the problem of cyber security, and market is the crucial driving force to improve cyber security. We must limited by the existing legal system.

With continuously development of mobile internet, big data and cloud computing, legislation of cyber security might repeat or conflict with existing law. Therefore government must value and encourage innovation of thought, technology and market of cyber security, and not limited by the content of existing legal system. The innovative content of cyber security legislation should break through framework of existing legal system and have forward-looking view.

Strengthening Ceaselessly International Collaboration of Cyber Security Legislation. In the speech in Brazil Parliament, President Xi Jinping pointed out that internet's development gives new challenge to national sovereignty, security, interests and every country's sovereign rights and interests in information area must not be infringed. International community should build peaceful, secure, open and cooperative cyber space together and set up multilateral, democratic and transparent management system of international internet.

The cyber security and law protection is new international topic. International community need adopt common legal regulation that is universally recognized and accepted, peaceful, secure, open and cooperative. There should be deeper research into the problem and how the existing international law to adapt to cyber space as well as actively exploration of new international norm adapted to cyber characteristics, including international standard of conduct and responsible national standard of conduct of information security. It is urgent to start international cooperation of legislation, vie for influence of China and inject Chinese elements in international cyber security legislation, make related international regulation within framework of United Nation, improve mutual belief and cooperation, maintain cyber peace and security and advance the internationalization, systematism and institutionalization together.

Conclusions

This work first researches the current international development state of cyber security. It is thought that cyber security is closely related to national security, and is a crucial topic in the face of all national governments. Later, the development of cyber security legislation and characteristics of cyber security strategy of U.S.A are studied. Based on the development situation of cyber security policy and legislation in China, the experience that can be referenced from those of America and adapted to Chinese practical environment is analyzed and summarized.

References

[1] The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [EB/OL]. [2011-05-06] / [2013-11-01]. http: // www.whitehouse.gov /sites/default/files/rss_vie-wer/international_strategy_for_cyberspace.pdf.

[2] The White House, National Strategy to Secure Cyberspace [EB/OL]. [2003-02-02] / [2011-11-01]. https: // www.us-eert.gov/reading _room /cyberspace_strategy.pdf.

[3] Liu Cheng-rui, Bi Jie, Comparison of Information policy between Japan and China and its enlightenment (in Chinsese), Journal of Library and Information Sciences in Agriculture. Vol.17, No.7 (2005): 32-34.

[4] Congressional Research Service, The 2013 Cyber security Executive Order: Overview and Considerations for Congress [EB/OL]. [2013-03-01] / [2013-11-01]. http:// www.fas.ort/sgp/crs/misc /R42984.pdf.

[5] Nakamura (Japanese), The role of government in network society: perspective of Japan's information policy (in Chinese), China Opening Herald. No. 7 (2001): 17-18