DOI 10.15302/J-SSCAE-2016.06.006

Improvement of the Cybersecurity Legal System in China

Li Yuxiao, Wu Hequan[2], Xie Yongjiang[3], Jiang Shuli[3], Cui Congcong[3], Mi Tienan[3]

1. Cyber Security Association of China, Beijing 100010, China
2. Chinese Academy of Engineering, Beijing 100088, China
3. Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Though the legislation of cybersecurity has witnessed some growth since the 18th National Congress of the Communist Party of China, there remains a significant gap between the construction of cybersecurity laws and the development of cybersecurity and informatization as well as the requirements of the public. Furthermore, there are problems related to legislation, enforcement, administration, and law-abiding consciousness. Some people, at home and abroad, question China's cybersecurity legislative efforts. Based on the analysis of current cybersecurity laws, the author suggests that the enactment of cybersecurity legislation must be expedited, especially with respect to cybersecurity law, e-commerce law, Internet information service administration law, personal information protection law, e-government law, information and communication network law, and cyber society administration law. Furthermore, the author suggests that these laws should be supported by matching regulations and enforcement mechanisms. Through these measures, China could establish a significantly improved legal system for cybersecurity.
Keywords: networks; Internet; cybersecurity; cybersecurity law; legal system

1 Introduction

Given the recent and rapid development and application of Internet information and communication technology, cybersecurity has become increasingly significant and complicated. Accordingly, the Internet should be regulated by laws. Governing cyberspace by law is key to protecting cybersecurity as laws generally elicit compliance through enforcement and disciplinary efforts. Currently, China's legal resources for cybersecurity are far behind the pace of cybersecurity development and informatization and are unable to adequately improve the legal system and protect individual rights in public society. In this paper, we will analyze the status and problematic aspects of the existing cybersecurity legal system and will offer suggestions to correct those deficiencies. In so doing, we expect to accelerate the development of China's cybersecurity legislation.

2 Concept and composition of the cyber legal system

2.1 Concept

A legal system encompasses all the legal departments which consist of related laws (documents) classified by certain principles and standards [1]. The cyber legal system is a unit that comprises all the lawful regulations moderating social relations related to the network. Such a system should be diverse enough to regulate all the cyber-based issues, but must also have a strict structure and compatible interrelationship in order to not only perform certain functions and indicate the national will of cyberspace regulation but also to ensure coordination between cyber law and other laws and maintain the harmonious unity of the national cyber legal system so as to guarantee satisfactory performance.

Received date: 20 September 2016; **revised date:** 15 October 2016
Corresponding author: Li Yuxiao, Cyber Security Association of China, Secretary General, Professor. Major research fields include Internet governance and cyberlaw. E-mail: liyuxiao@bupt.edu.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10).
Chinese version: Strategic Study of CAE 2016, 18 (6): 028–033
Cited item: Li Yuxiao et al. Improvement of the Cybersecurity Legal System in China. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.006

The cyber legal system is developed by particular cyber laws. Cyber law, as a product of the era of the Internet, differs significantly from civil and commercial law, administrative law, and economic law. Cyber law places the responsibility of constructing the system of rights and obligations in cyberspace—compensating for the shortcomings of traditional laws with respect to cyberspace—and attempts to regulate cyberspace orders. In addition to specifying rights and obligations of the subjects and regulating behaviors in cyberspace, the cyber legal system will constrict netizen self-administration and emphasize national security, public social interests, and cyberspace orders.

The cyber legal system is different from the cyberspace legal system. Cyberspace and cyber society is an extension of reality; thus, apart from cyber law, cyberspace law also includes other traditional laws applicable in cyberspace, such as civil law, criminal law, economic law, and administrative law, which together help maintain social order in cyberspace. Therefore, the cyber legal system is subject to the cyberspace legal system and not the other way around.

The cyber legal system is also different from the cyber legislative system. A cyber legislative system is a collection of all lawful documents, varying in scope and degree of force, which are devised by a legislative body at all levels in the course of designing national laws. This system is essentially composed of the sources of the law—perhaps better described as the outward manifestation of the law—embodied in the Constitution, laws, and administrative regulations, and local regulations [2]. The cyber legal system is also a collection of all cyber laws and regulations. Given that cyberspace is an extension of reality in the cyber domain, traditional laws are usually suitable in cyberspace; though some traditional laws require modification or improvements before they can be appropriately applied. Ergo, many cyber laws and regulations are mixed with traditional laws. Of course, due to the uniqueness of cyberspace, there are some special and separate cyber laws, including, for example, cybersecurity law and e-commerce law.

2.2 Composition

To study the inner structure of the cyber legal system is to study different functions and roles of the norms of cyber law. According to its theoretical logic, cyber law basically involves the Internet network subjects, behaviors, rights and obligations, and responsibility.

2.2.1 Lawful regulations of the Internet network subjects

The Internet network subjects mainly include: ① government, usually the cyberspace regulator; ② netizens, the largest Internet network subjects in number; ③ Internet association and community, the important units of cyber society, the latter of which has mushroomed in cyberspace; ④ Internet enterprises, the most critical subjects in cyberspace, such as service providers of Internet network platforms, information, access, and storage, and operators of telecommunications and online; ⑤ Internet intermediaries, which are important subjects of the Internet network markets, include testing organizations, electronic signatures certification and domain name registration organizations, and so on.

Lawful regulations of Internet network subjects mainly relate to the establishment, alteration, operation, and termination of Internet enterprises and other organizations, the accessibility of the market, and the identifying information of Internet network subjects.

2.2.2 Lawful regulations of Internet network behaviors

Internet network behaviors include: ① Internet network information behaviors, which produce, publicize, upload/download, gather, process, use, transfer, and delete information; ② Internet network transaction behaviors, including e-contracts and data exchanges; ③ Internet network intermediary behaviors, including certificating, monitoring, evaluating, and registering; ④ Internet network technology behaviors, which develop, maintain, update, operate, administrate, and protect the Internet network.

Lawful regulations of Internet network behaviors mainly relate to the establishment, validity, and legal consequences of Internet network behaviors.

2.2.3 Lawful regulations of Internet network rights and obligations

Lawful regulations of Internet network rights and obligations include: ① governmental authority and responsibility; ② netizens' rights and obligations; ③ the rights and obligations of Internet enterprises and other organizations.

2.2.4 Lawful regulations of Internet network responsibilities

Internet network responsibilities mostly involve Internet network civil liability, administrative liability, and criminal liability.

Based on the composition of current laws, the cyber legal system contains related cyber laws and special cyber laws. The former pertains mostly to Internet network-related laws and regulations formed by further application of traditional laws in cyberspace, such as lawful regulations of cyber violations and cybercrime. These cyber laws are developed by moderating and improving traditional laws such that they are applicable in cyberspace. The latter pertains mostly to particular laws for regulating social relationships in cyberspace. Due to the fact that traditional laws do not have comparable laws, special separate laws must be enacted and enforced. These laws consist mainly of cybersecurity law, personal information protection law, and e-commerce law.

3 The current cybersecurity legal system and its major problems

The cybersecurity legal system is a major part of the cyber legal system. It includes cooperative and multi-layer regulations of laws, administrative regulations, and department rules, which aim to protect cybersecurity. These laws and regulations involve mechanisms like cyber sovereignty and critical infrastructure protection, Internet network operation security, monitoring and early warning, and emergency disposal as well as cybersecurity and information security examination and Internet network subjects' rights protection. Cybersecurity laws have reached a critical stage in terms of the modernization of the national managing system as well as the ability of and reforms to the global Internet managing system. To secure national cyberspace, China must regulate behaviors threatening cybersecurity and promote the acquisition of new Internet technologies that will protect the sovereignty, security, and developing interests of China's cyberspace.

After China first gained full access to the Internet in 1994, it has experienced a gradual cognition shift regarding Internet management and cyber legislation. Initially, people regarded the Internet only as a technical tool. Accordingly, specifications like the Regulations of the People's Republic of China on Protecting the Safety of Computer Information Systems and the Interim Provisions on the Internet Administration of Computer Information Networks also treated the Internet merely as an emerging information technology. After 2000, people gradually began to realize that the Internet offered strong media properties, business opportunities, and social value. Accordingly, relevant specifications such as Telecommunication Regulations of the People's Republic of China and Administrative Measures for Internet Information Service have been issued one after another. In addition, all the departments began to emphasize and participate in the Internet information administration. Meanwhile, the Electronic Signature Law of the People's Republic of China motivated the development of e-commerce, and the Decisions of the Standing Committee of the National People's Congress on Preserving Computer Network Security also put an emphasis on cybersecurity. With the growing popularity of Internet applications, the Internet network has shifted from a virtual space to an indispensable part of real social life, opening a new page for China's Internet network socialization in an all-encompassing way. On February 27, 2014, the Office of the Central Leading Group for Cyberspace Affairs (hereinafter referred to as "the Central Leading Group") was established. Following its establishment, China developed a comprehensive method for governing Internet-related matters through inclusive coordination, top-level design, and cyber law. With the increasing needs of Internet administration, especially following the 18th National Congress of the Communist Party of China, China has made significant progress in cyber legislation.

According to the author's analysis, by August 2016, there were 45 cases of legal decisions related to Internet information, 53 cases of administrative regulations by the State Council, 58 cases of judicial interpretations, 115 cases of special ministry regulations related to Internet information, and 148 cases of special local laws and regulations related to Internet information. In other words, a system of cyber laws and regulations has begun to take shape in China, covering the fields of Internet network operation security, data security, and contents management; personal information protection; Internet network resources management, industrial management, and telecommunication services management; e-commerce; and cyber violation and cybercrime. Furthermore, industrial organizations, like the Internet Society of China, also developed over 20 self-discipline rules. Internationally, China plays an active role in participating and promoting international treaties related to the Internet network in order to secure national cyber sovereignty and national interests.

The National Security Law of the People's Republic of China, issued in 2015, and a series of other recent legislative practices, including cybersecurity law and e-commerce law (which are currently being drafted), indicate that China has accelerated the rate of cyber legislation. However, in terms of the cybersecurity legal system, it still suffers from some obvious vulnerabilities, which include: ① Current laws and regulations are not up to speed with Internet developments—Thus, they lack host laws and systematic architectural design; ② All levels of government and legislatures act on their own such that departmental and local legislation are not comprehensive, making it hard to adapt the features and rules of cyber laws; ③ The ability to enforce the laws is limited, lagging behind the enforcement needs; ④ Legislation emphasizes management over administration and obligations over rights, which minimizes China's ability to participate in international Internet affairs. ⑤ Talent related to cyberspace legislation is experiencing an extreme shortage, and the system for educating people and organizations about cyber laws is insufficient as well [3]. Thus, compared with efforts to accelerate cybersecurity legislation for protecting national interests in the United States and some developed countries in Europe, China lags behind. Furthermore, China's legal system requires additional improvements and advances.

In consideration of these issues, in February 2014, the Central Leading Group held an inaugural conference to coordinate a legislation schedule and improve laws and regulations involving Internet information management and critical information infrastructure protection. In October of the same year, the 4th plenary session of the 18th Central Committee of the Communist Party of China (CPC) approved the Decision of the CPC Central Committee on Major Issues Pertaining to Comprehensively Promoting the Rule of Law. It further suggested that Internet legislation should be enhanced to improve laws and regulations of Internet information services, cybersecurity protection, cyber society administration, and to moderate Internet network behaviors

through law. On April 19, 2016, General Secretary Xi Jinping pointed out in his speech delivered at a symposium on cybersecurity and informatization that China should accelerate cyber legislation development, promote lawful monitoring measures, and try to eliminate cyber risks. In July 2016, the 13th Five-Year Plan of National Informatization further emphasized the need to improve the informationized law framework with cyber legislation as the key feature in order to accelerate the development of a framework establishing laws and administrative regulations that aim to increase informatization development and underpin cybersecurity management. Officially, one of the key efforts in China's current legislation is to improve China's cybersecurity legal system.

4 Legislative recommendations on improving the cybersecurity legal system

Measures to improve the cybersecurity legal system should be based on the characteristics and rules of Internet network development, taking into consideration the legislative needs and combining special legislation and decentralized legislation. Thus, efforts should be made to evaluate, amend, improve, and supplement traditional laws and regulations that do not conform to the Internet context and to extend the applicability of these laws and regulations to cyberspace by way of legislative and judicial interpretation. In addition, China should take proactive measures to study new problems and situations in cyber society, to formulate specific legislation, and to deal with the governance challenges of cyberspace. Considering the current cybersecurity conditions, China should focus on enacting basic laws like the cybersecurity law, Internet information service administration law, personal information protection law, e-commerce law, and information and communication network law in the near future, duly enact e-government law and cyber society administration law, and issue supporting administrative laws and regulations based on the above laws.

4.1 Accelerate the enactment of cybersecurity law and ensure the security of cyberspace

The increasing dependence of the national economy and individuals' social lives on cyberspace places the cybersecurity issue in a prominent position. To adapt to new conditions and new issues related to national cybersecurity work, the Standing Committee of the National People's Congress added enacting cybersecurity-related legislation into the legislation program and annual legislation work plan for 2015. The second deliberation has already passed the draft of cybersecurity law and its enactment is forthcoming.

Cybersecurity law is the basic law for China's cybersecurity management. It defines top-level system designs, such as basic rules and strategic programs, that ensure cybersecurity, and builds and improves related fundamental systems in areas of cyber-physical security, cyber-operation security, cyber-data security, cyber-information security, and so on. Considering the current conditions and trends of China's cyberspace development, it is necessary to study and enact comprehensive laws regarding cybersecurity. Although facing an urgent legislative need for exploration and practice in cyberspace, China's study on the characteristics, rules, and development trends of cybersecurity is far from sufficient. That makes it difficult to formulate a law on cyberspace security through a single action or measure. Considering the primitive status of China's cybersecurity, we believe there is no need to cover all bases or demand perfection; instead we hope only to enact a cybersecurity law as soon as possible.

While formulating the cybersecurity law, China should expedite the process of studying and enacting laws and regulations that support cybersecurity. Such supporting administrative laws and regulations would include the cybersecurity level protection regulations, protection regulations for the security of critical information infrastructure, review regulations of cybersecurity, online protection regulations for minors, Internet network service regulations for cloud computing and big data, and protection regulations for the security of industrial Internet control system.

4.2 Enact Internet information service administration law and normalize the security management of Internet information

The form of Internet information services changes with each passing day, and, consequently, harmful and illegal information is readily available. Such information emerges endlessly and may include information that endangers national security, online prostitution information, online rumors, cyber defamation, information that imparts criminal methods, online suicide information, and cyber gambling information. Governments are seeking effective approaches to combat harmful Internet information. The State Council enacted Administrative Measures for Internet Information Service in 2000, which clearly lags behind media convergence and the development of Internet communication modes. Similarly, each department enacted related regulations for the management of information services in due succession based on its need to manage the information type and flow. Without a host law's guidance, regulations often overlap and conflict with each other. Accordingly, given this lack of internal connectivity, these regulations are in dire need of improvement.

Therefore, while learning from prior legislative experiences with law enforcement and administrative supervision of the Administrative Measures for Internet Information Service, China should enact the Internet information service administration law with the least possible delay and, in so doing, make clear each player's rights and obligations on the Internet information service market; promote the healthy and orderly development of Internet information service market; establish an Internet

information service supervision system and related mechanisms; define duties and powers of law enforcement departments; improve the liability system; implement effective punishment to guarantee deterrence against illegal and harmful Internet information; establish multi-party participating mechanisms; and effectively combine government regulation and law enforcement with public and non-governmental organization oversight.

Western media has always criticized and disparaged the management of Internet information service in China. In essence, the cultural and systematic differences between China and western countries cultivate the differences in information service modes and supervision methods in the cyber environment—each country applying their normal practices to protect their own culture and civilization. The Internet information supervision practices in China have not restricted the spread and development of the Internet; instead, they have spawned the world's largest Internet network infrastructure and community as well as the most dynamic network service market. More and more countries are adopting and acknowledging China's Internet development experience, demonstrating that these practices are in accord with China's need for development and, thus, that the cybersecurity legislation should be based on China's need for development.

4.3 Formulate personal information protection law and protect the security of citizens' personal information

Personal information presents an important and strategic asset in the big data age, as it not only possesses commercial value but also involves national security and social public interests. The lack of protections for personal information rights in a cyber environment is a major challenge that the whole world must confront. Driven by interest, actions like illegal collection, trading, and stealing of personal information, which cause financial loss to netizens and even threaten people's lives, continue despite repeated prohibition.

It is important that the cybersecurity law ensures personal information rights. Existing laws in China have made relatively significant progress in protecting personal information rights. Some laws have already established a legal framework for personal information protection, which includes criminal liability, administrative liability, and civil liability under such laws and regulations as the Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks, Criminal Law of the People's Republic of China, Law of the People's Republic of China on Resident Identity Cards, and Law of the People's Republic of China on the Protection of Consumer Rights and Interests. In particular, the Amendment (IX) to the Criminal Law of the People's Republic of China has further strengthened the protection of personal information through criminal laws. However, the environment for protecting personal information has no sign of marked improvement, and actions that infringe on personal information rights, such as illegal collection or trading of personal information and telecom fraud, are common. The reason such actions are common is the threshold to initiate a criminal protection mechanism is high and civil remedies are troublesome—As it is difficult to collect evidence and the cost of seeking such remedies are high. Furthermore, powerful administrative protection mechanisms have not been fully established, which makes breaking the law an inexpensive venture and essentially encourages the behaviors that infringe on personal information rights.

Personal information rights are fundamental rights of citizens, and these rights should be legally acknowledged and protected. It is necessary to enact a law that systematically protects personal information as soon as possible and to establish the information subject's rights and the rights, obligations, and responsibilities of subjects in the following processes: personal information collection, storage, processing, utilization, transmission, and so on. In the event that civil protections are ineffective, effective administrative personal information protection mechanisms should be built through legislation to timely stop the spread of behaviors that infringe on personal information rights, to protect personal information practically and effectively, and to maintain netizens' confidence and trust in Internet use.

4.4 Enact e-commerce law and ensure the security of e-commerce transaction

Recently, e-commerce has developed rapidly in China. While it has played a positive role in creating new consumer demands, triggering a new round of investment booms and new channels for increased employment and income while promoting transformations and improvement in the service and manufacturing industries, it has also generated a lot of chaos—allowing people to sell fake commodities, swindle consumers, and participate in unfair competition. Accordingly, e-commerce is in dire need of legislative regulation.

The e-commerce law sets out the legal standard for and the relevant elements of the commercial process with the aim of promoting the sustainable and sound development of e-commerce, rectifying the market order, and ensuring each player's legal rights in e-commerce activities. It covers important systems of e-commerce market access, e-contracts, e-payment and logistics, data information protection, consumer protection in e-commerce, platform responsibility, cross-border e-commerce, and so on.

The sustainable development of e-commerce could not exist without secure transactions, and, therefore, one of the fundamental elements of the e-commerce law is ensuring secure transactions. Many parts of e-commerce are involved in ensuring that transactions are secure, including identity authentication, validity of e-contracts, logistics security, payment security, market order of e-commerce. Each of these aspects of e-commerce should be defined through legislation. The e-commerce legislation process,

which was launched in December 2013, should be accelerated, and efforts should be made to ensure that the legislation is adopted during the current National People's Congress's term.

4.5 Enact information and communication network law and ensure the security of the allocation, construction, operation, and transmission of Internet information sources

Traditional telecommunications and broadcasting law systems are mutually independent; in fact, barriers have been formed that prevent them from integrating. The three major administrative laws and regulations—Regulations on Broadcasting and Television issued in 1997 and Regulations on the Protection of Radio and Television Facilities and Telecommunication Regulations of the People's Republic of China issued in 2000—are lagging severely behind the development needs of broadcasting, television, and telecommunication industries. Furthermore, they are unable to meet the demand for the "integration of three networks." The further enactment of the Telecommunication Law and the Protection Law of Radio and Television Transmission would hinder the advance of network integration. With the ever-increasing trend of network integration, readjusting the current legal system to adapt to the development of network integration is an urgent need. At present, China does not have a superior law that regulates the integrated cyberspace of three networks. Thus, it is imperative to formulate a unified law on information and telecommunication networks that stipulates the basic laws and regulations regarding subjects, behaviors, rights, and responsibilities in Internet, telecommunication, broadcasting and television, and other information and telecommunication markets in cyberspace.

As one of the basic laws of cyberspace, it is inappropriate for the information and communication network law to include the content of separate legislative drafts, such as cybersecurity, e-commerce, e-government, Internet information service, personal information protection, and so on. It is recommended that priority should be placed on regulating the development, construction, and operation of Internet network facilities and assets; building fair, reasonable, and effective systems for allocating and utilizing Internet network resources; and building unified supervisory systems.

4.6 Duly enact e-government law and ensure the security of e-government and government data

At the end of the 20th century, China began implementing e-government. Guidance from the leading group of national informatization on the establishment of China's e-government was issued in 2002, promoting a development boom of government informationization in China and playing a significant role in guiding the construction of China's e-government. However, that guidance was issued at a time when China's e-government construction was in its infancy, and, at that time, its priority was placed on regulating the informatization construction of critical industries, ignoring the importance of creating a government portal website. The Administrative License Law of the People's Republic of China [4], issued in 2003, is the earliest law that legally approved e-government, but its regulations are not complex enough to handle all the issues that may arise. Other regulations regarding e-government are seen in departmental rules, local laws and regulations, and other regulatory documents. In general, China lacks a special law or regulation that regulates e-government affairs; thus, an integrated e-government legal system has yet to be established. The delay in e-government legislation severely impedes the development of e-government and the economy that relies on e-government.

China should duly enact e-government law, but before that, it should issue regulations on e-government and amend the Regulations of the People's Republic of China on the Disclosure of Government Information. Basic policies of informatization, information disclosure, information sharing, and information security in the e-government domain should be established in order to safely control the acquisition, transmission, storage, utilization, and disclosure of government data. Also, the scope and operation methods of all departments for data sharing should be defined as well as the rights and obligations of different departments for managing and sharing data. By guiding and promoting the development of e-government, China can promote innovation and entrepreneurship that relies on government data.

4.7 Duly enact cyber society administration law and maintain an orderly cyber society

Cyber society is essentially the social relationships formed by different interweaving networks among different people. "As a historical trend, the dominant function and process of the information age are increasingly being organized by the Internet network. The network has built a new social form for China's society, and, in addition, the proliferation of networking logic has substantially changed the operations and outcomes with regard to production, experience, power, and culture. The network situation of social organizations already exists in other time and space, and the new information technology paradigm provides a material basis for its penetration and expansion throughout the social structure [5]."

Nowadays, the network influences trends and goals of China's society, posing far-reaching impacts on individuals, organizations, and China's society as a whole. The changes that the network has brought to social structure and the way people behave is obvious, and the networking of communities poses difficulties in social management. Currently, it is imperative for China to recognize the importance of studying cyber society and to duly enact cyber society administration law after issuing some administrative regulations to guide and regulate the sound development of cyber society.

5 Conclusions

We explore how cybersecurity is governed by law based on China's previous experiences of Internet governance, concluding that the foundation for virtuous and sustainable development of China's society is to administer cybersecurity through law, even if there is industry-based self-discipline or sectoral supervision. China's cybersecurity legislation should ensure national sovereignty, citizens' personal information rights, and information security in cyberspace, which are the starting points and reference standards of its legislation. Many countries share a common goal of maintaining cybersecurity through proper cyber legislation as it accords with most countries' interests and is consistent with society's demand for development and progress.

References

[1] Shen Z L. Jurisprudence [M]. Beijing: Beijing University Press, 2014. Chinese.

[2] Zhang W X. Jurisprudence [M]. Beijing: Higher Education Press, Beijing University Press, 2011. Chinese.

[3] Xie Y J, Jiang S L. Analysis of the situation and problem on the legislation of cyberspace in China [J]. Chinese Journal of Network and Information Security, 2015, 1(1): 24–30. Chinese.

[4] Zhang H. Present situation and development suggestions of E-government legislation in China [J]. Chinese Public Administration, 2007 (11): 24–26. Chinese.

[5] Castells M. The rise of the network society [M]. Beijing: Social Sciences Academic Press, 2006. Chinese.