Daoli Huang

Research on the Rule of Law of China's Cybersecurity

China's Rule of Law in Cybersecurity Over the Past 40 Years

華中科技大學出版社
http://www.hustp.com

Springer

Research on the Rule of Law of China's Cybersecurity

Daoli Huang

Research on the Rule of Law of China's Cybersecurity

China's Rule of Law in Cybersecurity Over the Past 40 Years

華中科技大學出版社
http://www.hustp.com

Springer

Daoli Huang
The Third Research Institute
of the Ministry of Public Security
Shanghai, China

ISBN 978-981-16-8355-8 ISBN 978-981-16-8356-5 (eBook)
https://doi.org/10.1007/978-981-16-8356-5

Jointly published with Huazhong University of Science and Technology Press
The print edition is not for sale in China (Mainland). Customers from China (Mainland) please order the print book from: Huazhong University of Science and Technology Press.
ISBN of the Co-Publisher's edition: 978-7-5680-1465-6

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Editorial Committee

Foreword

Since the Report on the Work of the Government of 1978 proposed energetically developing emerging science and technology, particularly to expedite the research of integrated circuits and electronic computers and stimulate their popularization and application, China's Internet industry has developed for more than four decades. Over these four decades, the network security and informatization business of China has set an impressive record of achievement.

The evolution of the Chinese Internet industry for more than four decades precisely keeps track of the historical development of the cybersecurity legal frameworks of China. Especially since the 18th National Congress of the Communist Party, China's legal construction in cybersecurity has developed in leaps and bounds, and the legal regimes that focused on the Cybersecurity Law of the People's Republic of China likewise have matured. As the first batch of scholars studying cybersecurity law, I have witnessed the twists and turns in the development of China's cybersecurity legal regimes from scratch, from weak to strong and from passive to active. I am deeply aware of the ups and downs of the development process and sincerely feel gratified for China's achievements today.

However, in the vigorous development of cybersecurity law-based governance, many researchers were eager to explore the future development path and lacked an overall grasp of the history and evolution of cybersecurity legislation in China. As a result, their research was just like a rootless tree, and even worse, misunderstood China's cybersecurity legislation and misjudged the development path.

In 2017, my student Huang Daoli, the editor-in-chief of this series, told me that she planned to publish a series of books to review China's cybersecurity legislation systematically. Meanwhile, she also conveyed colleagues some insights, prejudgments on its future and compliance opinions of our team in the domain of cybersecurity in which she has been engaged for more than 30 years. I fully agree with her in this regard, but I also know that it is not so easy. To the best of my knowledge, the process of writing this series is beset with numerous difficulties. Researcher Huang Daoli also asked me for advice many times. During this time, they specially organized seminars and invited relevant legislators to tell the stories behind the legal provisions.

This pragmatic attitude also makes me profoundly confident and expectant for the publication of the series, which is also the story behind these books.

The first time I read the final draft, I came to realize that Chinese academic circles have been exploring and working on cybersecurity as a new realm of jurisprudence for more than four decades, and it has been more than 30 years since I started studying cybersecurity legislation in 1988. Apart from feeling the passage of time, my thoughts are also touched overwhelmingly. In 1978, the new period of reform, opening up and socialist modernization unfolded, which kept almost the same pace as the global commercial popularization of the Internet. In 1978, the Report on the Work of the Government put a high premium on the development of integrated circuit and electronic computer technology, which not only laid the foundation for the development of China's information technology industry but also made China quickly aware of the possible security threats posed by the application of this new technology. As early as 1981, China's public security departments found that computer equipment was exposed to the risk of data leakage through information reproduction. The central government attached enormous importance to this and required the establishment of laws and regulations to ensure that there are laws to abide by to secure China's computer information systems. In 1982, China began to launch legislative research on the security protection of computer information systems, gradually exploring the road of law-based governance in cybersecurity. By 1994, Decree No. 147 was promulgated and implemented as the first cybersecurity legislation in China. This landmark legislative case has initiated a new era in China's construction of law-based governance in cybersecurity.

There is no denying that over a long period of time, the emphasis of China's legal construction in cybersecurity has always failed to break through the limitation of "computer room thinking." Specifically, legislation chiefly focuses on the security of computer information systems, which still bears little resemblance to the cybersecurity we understand today. Of course, this is compatible with the level of technological development at that time, which is also the result of "stability" and "lag" of the law itself. After 2000, China's informatization construction began to develop at top speed, and information technology has been applied extensively on a social scale. The national level attaches more importance to information security as well. In July 2003, the Information Office of the State Council entrusted me to study the information security laws, regulations and law enforcement to offer theoretical research support for the Network Information Security Regulations included in the plan for legislative work of the State Council in 2003. In April 2004, the seminar on Information Security Legislation organized by the Information Office of the State Council was held at Xi'an Jiaotong University. The participants included representatives of crucial industries, ministries and commissions of the State Council, representatives of important enterprises, etc. The theme of the seminar was to probe into the major issues in the domain of information security in China at that time and the ideas of response to legislation. At the seminar, collective demonstration and acceptance of the results of my project were launched as well.

In the years that follow, information technology begins to integrate into the fabric of society and is almost indistinguishable from society itself. After the

digital economy has turned into a new "motive power of development," information technology has made increasingly obvious contributions to the progress of modern society, but this contribution still comes at a cost—we are more dependent on the security of technology and technology utilization activities than ever before—"dependence" is objective. In the realm of jurisprudence, this renders information technology-based social relations, an independent adjustment object, and escalates cybersecurity to be a comprehensive issue involving the country, industry and individuals.

With respect to this series of books, several highlights and breakthroughs deserve affirmation and praise. Existing studies generally regard Order 147 as the beginning of China's network security legislation; nevertheless, the legislative motion before Decree No. 147 and its historical backgrounds are basically a blank area of research. It is indeed a breakthrough of great practical significance to integrate the development of China's reform and opening up with the legal construction of Chinese cybersecurity legislation, which tremendously broadens the horizon of tracing to the sources of cybersecurity law and makes the study of rule of law in cybersecurity closer to the technological approach.

The current international situation is turbulent and changeable. In the context of "technology decoupling" and "deglobalization," China is drawing up an important plan for supply-side structural reforms, actively developing strategic industries while stabilizing traditional industries, in a bid to avoid the dilemma of "strategic dependence" of core technologies for a long time, raise the level of science and technology, forge core competence and engage in and lead the reconstruction of global industrial chain. Since the enforcement of the Cybersecurity Law of the People's Republic of China for more than four years, China's network information work has broken new ground, achieved new development and opened up a new situation, which fundamentally advances China's transition from "a large cyber country" to "a cyber superpower," providing a vital legal basis for cyberspace governance in accordance with the law, and promotes China's comprehensive management capacity of cybersecurity continue to improve. Looking into the future, quite a number of problems in the legal system of cybersecurity await further perfection.

May the author and colleagues in academic circles can contribute more wisdom to the research of cybersecurity laws.

Here is the Foreword above.

Shanghai, China
September 2020

Ma Minhu
Professor of Xi'an Jiaotong University
Director of Suzhou Institute of
Information Security Law
Xi'an Jiaotong University

Introduction

The Fourth Industrial Revolution marked by big data, cloud computing, unmanned driving, AI and 5G is sweeping across the globe. The digital and intelligent revolution has not merely influenced individuals' living conditions and lifestyles at the micro-level but has altered the production organization mode, national order, international situation and even the world pattern at the macro-level. The expedited integration of the cyber world and the physical world has also spawned and amplified the risk effect of cybersecurity upon which social digital technology relies. On February 27, 2014, General Secretary Xi Jinping clearly stated at the first meeting of the Central Leading Group for Cybersecurity and Informatization that "without cybersecurity, there will be no national security, and without informatization, there will be no modernization." China officially launched a series of top-level designs and plans for the purpose of building China into a national power in cyberspace. In the context of national development, building an all-round rule of law system of cybersecurity is of primary importance in cybersecurity work.

In retrospect, New China's development in the past 40 years of reform and opening up is of unique and extraordinary historical significance. From the historic decision of "tightening up the socialist legal system" made at the Third Plenary Session of the Eleventh Central Committee in 1978, to the time when the 19th National Congress of the Communist Party of China further promoted adhering to "law-based governance of the country" as the basic strategy for upholding and developing socialism with Chinese characteristics in the new era, the magnificent 40-year socialist legal system with Chinese characteristics is also the 40-year innovation and reform of cybersecurity rule of law in China. China has seized the historical opportunity offered by the development of informatization to the country and people; focused on the theme of security and development, it has realized the continuous perfection of rule of law in cybersecurity from scratch, from fragmentation to systematization and from response to prevention and embarked on a path of rule of law in cybersecurity that is both in line with international practices and with Chinese characteristics. Currently, China's comprehensive governance pattern of network co-construction, co-governance and sharing has basically taken shape, which has scored impressive achievements and put to the test of history.

Research on the rule of law inside cybersecurity is a major issue of the times brought by the development of information technology. The study of rule of law in cybersecurity poses enormous challenges, taking on prominent interdisciplinary characteristics, which requires strategic, holistic and forward-looking innovative thinking, and finally tests the legal personnel's capability to get to a grip on society and adapt to social changes. As a generation born after the reform and opening up and growing up with it, I was admitted to the major of Economic Law, Xi'an Jiaotong University in September 2003 and started my postgraduate studies. I have studied under Professor Ma Minhu and listened to his teachings to this day. Professor Ma Minhu is one of the founders of research on information security law and founded the Information Security Law Research Center, Xi'an Jiaotong University, the first academic institution specializing in research on information security law in China. During my academic career, I engaged in the research project entrusted by the legislation of Network Information Security Regulations of the former Information Office of the State Council, and some research findings were written into the Research on Information Security Law (published by Prof. Ma Minhu in 2004), China's first monograph that systematically studies the basic theory of information security law. Thanks to the research foundation and support of my supervisor and seniors, I can launch related research and academic exploration from a comparatively high starting point. In June 2007, I joined the Third Research Institute of the Ministry of Public Security and began to work as a people's police engaged in cybersecurity. As a legal person on the front of public security science and technology, the study of rule of law in cybersecurity is the objective need of implementing the practice of comprehensively governing the country in accordance with the law and the requirements of public security work in the new era, and it is also a professional and personal feeling derived from teachers' instructions.

Over the past four decades of reform and opening up, China, like other countries throughout the world, has been increasingly confronted with complex and changeable cybersecurity issues. The change of social form described in the Third Wave, Being Digital or the Rise of the Network Society, is becoming a reality, and the change of legal paradigm of cybersecurity in China is precisely unfolding in this process. Officially enforced basic laws, such as the Cybersecurity Law of the People's Republic of China, the Cryptography Law of the People's Republic of China, the National Security Law of the People's Republic of China and the Counterterrorism Law of the People's Republic of China, the Data Security Law and the Personal Information Protection Law, have jointly constructed a Chinese legal assurance system of cybersecurity characterized by more coordinated horizontal internal systems, a wider external radiation scope and more three-dimensional longitudinal systems, principles and rules. In the course of nearly 20 years of academic research, a large number of my academic research findings are also closely associated with these legislations. Moreover, thanks to the support of my Supervisor and the Third Research Institute of the Ministry of Public Security, I have attained the value goal of applying scientific research findings directly to legislation on cybersecurity, which has been fully recognized by national and local institutions such as the Legislative Affairs Commission of the Standing Committee of the National People's Congress, the State Cryptography

Administration, Cyber Security Department of the Ministry of Public Security, Legal Affairs Bureau of the Ministry of Public Security and the Office of the Leading Group for Big Data Security of Guizhou Province. At the moment, I and the team of the Cybersecurity Law Research Center of the Third Research Institute of the Ministry of Public Security are serving the needs of the work of the cybersecurity center, fully integrating social forces such as universities, scientific research institutions, cybersecurity associations and Internet enterprises and other social forces and conducting extensive academic exchanges to jointly explore the future direction of cyberspace security governance in China. We have made persistent endeavors in the research, drafting and revision of subordinate administrative regulations of the cybersecurity law, such as the Regulations on the Classified Protection of Cybersecurity and the Regulations on the Security Protection of Critical Information Infrastructure, and the formulation of the guidelines for the administrative law enforcement of cybersecurity.

The series of books published this time—the Review Volume of Research on China's Rule of Law in Cybersecurity: Zhongguo Wangluo Anquan Fazhi 40 Nian, the Trend Volume of Research on China's Rule of Law in Cybersecurity: Research on the Rule of Law of Cybersecurity 2020 and the Compliance Volume of Research on China's Rule of Law in Cybersecurity: Analysis on the Law of Cybersecurity 2020—outline the prospect of cybersecurity rule of law in China from different dimensions. From the point of view of the reality of the rule of law, the Review Volume presents the development course of the 40-year construction of the cybersecurity rule of law in China. From the point of view of academic research, the Trend Volume brings together some research findings on the legal issues of cybersecurity, such as data governance, legal regulation of security vulnerabilities, personal information protection, protection of critical information infrastructure security and forensics and authentication of electronic data, in recent years. From a practical point of view, the compliance volume shows Yuan Hao's understanding of cybersecurity compliance and reflection on legal rules at a higher level as a professional lawyer.

The Review Volume of Research on China's Rule of Law in Cybersecurity: Zhongguo Wangluo Anquan Fazhi 40 Nian divides the legalization process of China's cybersecurity into three stages: security governance of network tools, security governance of network society and security governance of network country. By sorting out the cybersecurity policies and laws in different stages as well as their development trends, it well reflects the evolution process of the rule of law on the strength of the technical application scenarios, which provides valuable basic data for legal construction development in cybersecurity and offers crucial practical value. In the face of such a grand task—research on the 40-year history of cybersecurity legal construction in China—we not only need to gain a profound understanding of China's Internet industry but also have an accurate command of the evolution and essence of China's cybersecurity legal regimes. This is indeed not easy for the writing team. Fortunately, we have received unreserved guidance from Prof. Ma Minhu and many seniors of the Expert Committee of China Information Security Law Conference in this work. Here, we sincerely express our gratitude: Thank you!

Looking ahead, China's opening up is offering new avenues and presenting new opportunities to nations around the world. Faced with the profound changes in the

world today, it is the responsibility and dream of all cybersecurity legal persons to accelerate the building of a model of comprehensive law-based governance, to explore China's plan for cybersecurity regulation on the basis of international experience and domestic practice, to transform the effectiveness of Chinese law-based model building into real governance efficiency, to maximize the digital well-being of the country, society and individuals and finally to fulfill the modernization of national governance capacity. The realization of these dreams still requires the exploration and struggle of all colleagues, which is also the essence of my team's perseverance.

What's past is prolog.

The year 2021 is destined to be an extraordinary year. Thanks to Guo Shanshan and her editorial colleagues from Huazhong University of Science & Technology Press, we have gone through the epidemic and headed for the future hand in hand! I hereby express my heartfelt thanks to Yuan Hao, He Zhile, Hu Wenhua, Liang Siyu, Ma Ning, Zhao Lili and other editors who worked with me. Let us set sail again and work for a glorious future with our united efforts!

The editors of this series are limited in talent and learning, so we dare not say anything about the value of the series. However, I wish that the publication of this series will be a boon to the study of cybersecurity rule of law in China in the future.

Daoli Huang
Researcher of the Third Research Institute
of the Ministry of Public Security
Secretary General of the Expert Committee of China
Information Security Law Conference

Contents

Chapter 1
40 Years of China's Legal Construction in Cybersecurity

In 1978, China entered the new era of reforming and opening up and socialist modernization construction. In that year's Report on the Work of the Government, it was proposed to energetically develop emerging science and technology, particularly to expedite the development of research on integrated circuits and electronic computers and to apply them extensively in all aspects. To date, China's Internet industry has developed for more than four decades. The development of the Internet industry for more than four decades is the history of China's legal construction in cybersecurity and the exploration history of maintaining a balance between development and security.

On September 14, 1987, Beijing sent China's first e-mail, launching the prelude to China's use of the Internet. On April 20, 1994, the demonstration network project of education and scientific research in the Zhongguancun area was implemented through the 64 K international dedicated line connected to the Internet by Sprint Company of the United States, and China became the 77th country with a fully functional Internet on a global scale. The opening of the international dedicated line was a huge milestone in the development of China's Internet industry. Since then, China has officially started to take the path of informatization construction.

Over the past four decades, the application of the Internet in China has gradually infiltrated into all aspects of society, such as politics, economy, military, culture and business, from a few fields, such as computer, education and scientific research, in the early stage. Driven by the "Internet +" wave, China has gradually moved from "following" to "running alongside" in information technology innovation, platform economy development and new business forms and new applications, and in some areas, China has "taken the lead in race". In the past 40 years, the Internet has approached average households from minority groups in individual fields, and China has taken first place worldwide with respect to the number of cyber citizens, becoming a veritable large cyber country. Over the past four decades, China, like other countries throughout the world, has been increasingly confronted with complex and changeable cybersecurity issues. Faced with such threats and risks as raging computer viruses, frequent network attacks, rampant illegal and criminal network activities, and

D. Huang, *Research on the Rule of Law of China's Cybersecurity*,
https://doi.org/10.1007/978-981-16-8356-5_1

deviated ecological governance of networks, China constantly explores the balance between security and development while stimulating the development of Internet construction at top speed. In the past 40 years, China's rule of law in cybersecurity has undergone many changes. Along with the perfection of legal system from Decree (No. 147) of the State Council in 1994, the Regulations of the People's Republic of China on the Security Protection of Computer Information Systems, to the Decision of the Standing Committee of the National People's Congress on Guarding Internet Security in 2000, and then to the Cybersecurity Law of the People's Republic of China in 2016 (hereinafter referred to as Cybersecurity Law) as well as its supporting laws and regulations, China's rule of law of cybersecurity has undergone changes from security governance of network tools, security governance of network society to security governance of network country, realizing the transformation from scratch, from fragmented legislation to systematic legislation, and from extensive legislation to refined legislation.

1.1 Cyberspace Governance in the View of Equipment Security

1.1.1 Legislative Background

At the beginning of the application of information technology, China began to realize the significance of information technology and informatization for national security and economic construction. At this stage, China worked hard to change the traditional opinions of information technology, making the national decision-making bodies and crucial industries realize that science and technology, especially computer information technology, can be extensively applied in traditional administrative areas to improve the management system and raise the level of modernization. At this stage, the government exerted the leading role in researching and popularizing computer technology, which was regarded as a tool to enhance the national management level. The computer applications spawn as a result are chiefly concentrated in education, scientific research, government and other crucial areas, and the basic operations of the network are conducted by public networks, education networks, science and technology networks, economic and trade networks and other industries.

With regard to economic construction, China launched the great new revolution of reform and opening up in 1978 and entered a new era of socialist modernization. Upholding the idea that only when the country is strong can it truly assure security, China has begun to put a high premium on the development and application of science and technology. In 1978, the Report on the Work of the Government proposed catching up with the ever-changing pace of modern science and technology with the least delay possible, energetically developing emerging science and technology, particularly expediting the development of research on integrated circuits and electronic computers and making them extensively used in all aspects. In 1985, the Central

Committee of the Communist Party of China released the Decision on the Reform of Science and Technology System, emphasizing that economic construction must be on the strength of science and technology, and scientific and technological work must be oriented to the strategic policy of economic construction. In 1986, China came up with the National High-Tech Research Development Plan (i.e., "863" Plan). As a strategic plan, it is linked with information technology, including communication technology, information acquisition and processing technology, and automation technology of computer integrated manufacturing systems and intelligent robot themes. In August of the same year, Wu Weimin of the Institute of High Energy Physics, Chinese Academy of Sciences, through satellite connection, remotely logged into the account of Wang Shuqin in a machine VXCRNA in CERN, Geneva, on an IBM-PC at 710 Beijing Institute and sent an e-mail to Steinberger in Geneva.[1] However, this email was sent only by remote login and controlled by computers thousands of miles away, without forming a data exchange protocol between computers.[2] In September 1987, with the help of the research team led by Professor Werner Zorn of Karlsruher Institut für Technologies in Germany, Professor Wang Yunfeng and Dr. Li Chengjiong set up an e-mail node in the Beijing Institute of Computer Applications (ICA) and successfully sent an e-mail to Germany on September 20th, with the content of "Across the Great Wall we can reach every corner in the world".[3] As a result, the first e-mail was born in China.

Since the reform and opening up, China's inbound and outbound goods and articles have increased in large quantities. It was difficult to satisfy the actual demand of business volume processing by simply increasing the number of business personnel in the customs system. Since the mid-1960s, developed countries have set out to study the computer application of customs. During the "7th Five-year" Plan, the State Council established the construction of 12 crucial electronic information and business systems, including the national economic information system, public security, railway, civil aviation, meteorology, banking, and other information systems.[4] In March 1993, Zhu Rongji, then Vice Premier, presided over the meeting and proposed and planned the construction of the China Golden Bridge Network (referred to as the ChinaGBN Project). In August of the same year, Premier Li Peng approved the use of prime minister reserve funds, totaling $3 million, to support the start-up of ChinaGBN preproject construction.[5] At the end of 1993, the Three Golden Projects, the initial project of China's national economy informatization, was officially launched, namely, the ChinaGBN Project, Golden Customs Declaration Project

[1] Memorabilia of Internet from 1986 to 1993. http://www.cac.gov.cn/2009-04/10/c_126500533.htm.

[2] China's bumpy Internet access path: the Internet coming out of the narrow path. http://www.isc.org.cn/ftfy/ft/listinfo-13329.html.

[3] Memorabilia of Internet from 1986 to 1993. http://www.cac.gov.cn/2009-04/10/c_126500533.htm.

[4] Gang [1].

[5] Memorabilia of Internet from 1986 to 1993. http://www.cac.gov.cn/2009-04/10/c_126500533.htm.

and Golden Card Project, which is intended to build China's "information quasi-high-speed national highways"[6] and raise the informatization level of the national economy from infrastructure construction, foreign trade and finance. During the construction of these information projects, China realized that only by improving the networking degree can computers achieve high-level application development.

In April 1994, China's NCFC project was opened through the 64 K international dedicated line connected to the Internet by Sprint Company of the United States, realizing full-function connection with the Internet, and China was officially recognized as the 77th country with full-function Internet internationally. In May 1994, the Institute of High Energy Physics, Chinese Academy of Sciences set up the first WEB server and launched the first set of web pages in China. In addition to introducing China's high-tech development, there was also a column called "TourinChina". Meanwhile, the National Research Center for Intelligent Computing Systems opened Shuguang BBS Station, the first BBS station in mainland China. In August 1995, the ChinaGBN Project was initially accomplished, and networking (satellite network) was opened in 24 provinces and cities, which was connected with international networks. In December of the same year, the "100-Institute Networking" Project of the Chinese Academy of Sciences was accomplished.[7] China has gradually entered the preparatory stage of Internet development.

In the realm of safety control, under the impetus of the development of computer science and technology, social and national security issues became complex and changeable along with the popularization of computer and networking applications in the early 1980s. Thereafter, Western developed countries adopted network security defense countermeasures in succession. Upon investigation, it was found that computer security turned into a topic of prominence in the international community. Sweden, the United States, Canada, Britain, France, Germany and other countries worked out or set up specialized legislation and research institutions. The United Nations set the IFIP/CSTC, which held an international conference on a yearly basis. Restricted by the ideology and Paris Coordinating Committee of NATO, computer technology has not yet been popularized and applied in socialist countries. China recognized that although domestic computers had just started and domestic computers were still in the experimental stage of research and development, the popularization and application of computers had proven to be an inevitable trend, and national and social security issues in the international community would also apply to China. If there were no sound precountermeasures, there would inevitably be potential security risks in building information infrastructure and setting up Internet applications in China with computing devices exposed to numerous hidden safety hazards.

To address the potential threats to national security imposed by information technology, the central government took three strategic measures: ① set up special departments to stimulate the development of information technology; ② establish laws and

[6] https://baike.baidu.com/item/ThreeGoldenProjects/106799?fr=aladdin.

[7] Memorabilia of Internet from 1994 to 1996. http://www.cac.gov.cn/2009-04/11/c_126500497.htm.

regulations and enact legislation to ensure that there are laws to abide by in the security work of China's computer information system; and ③ crack down upon information crimes and promote security and development simultaneously.

In 1983, the Chinese public security unit set up a computer management and supervision institution—Public Information Network Security Supervision Bureau[8] (Computer Administration and Supervision Bureau of the Ministry of Public Security), which was provided with two functions: first, planning and building the computer network system for public security, boosting the informatization and modernization of public security business, and forming and summing up the practical experience of computer security in China simultaneously; second, studying and judging the dynamics and trends of computer security at home and abroad, and working out national and social countermeasures for public security with Chinese characteristics. In addition, to ensure that the state has laws to abide by and rules to follow in protecting the computer information system as well as its associated networks, in 1982, China set up about launching legislative research around the security protection of computer information systems and gradually explored the construction of the cybersecurity rule of law in China with emphasis on equipment safety. After several years of investigation, analysis and legislative planning, it was recognized that China shall first set up the basic management system of computer security. In 1986, the Ministry of Public Security drafted China's first computer security regulation and began to solicit opinions extensively, which were reported to the Ministry of Public Security, the Legal Affairs Office of the State Council and the Standing Committee of the State Council for examination and verification level by level. During the period of examination, with respect to the legislation hierarchy, the State Council considered that computer information security is a newly emerging thing that shall be coarse rather than fine, so it is more prudent to introduce administrative regulations first, leaving room for the later development of the computer industry and system adjustment. It is advisable that the administrative regulation system shall be upgraded to law with solid social practice experience after a certain period of enforcement.

Throughout this process, computer viruses and special computer crimes had been increasingly rampant in all parts of the country, although computers in China were still in the stage of stand-alone application and a computer network had not yet taken shape. In July 1986, the case in which Chen, an accountant of Shekou Subbranch, Shenzhen Branch of Bank of China, and Su, an accountant of Dongmen Subbranch, Shenzhen Branch of Bank of China, jointly stealed customer deposits via computers, was solved, and it was the first computer-related crime discovered in China.[9] In 1988, China discovered the first computer virus since the founding of New China, that is, bouncing ball virus. The virus influenced the running efficiency of computer

[8] In 2008, the Public Information Network Security Supervision Bureau of the Ministry of Public Security was renamed as the Cyber Security Department of the Ministry of Public Security, and the cybersecurity teams of local public security departments were set up successively.

[9] Analysis of the Development Trend of Computer Crimes. https://www.docin.com/p-6041481.html.

software, with instant widespread accessibility. Since then, large-scale viruses such as 64 virus, Michelangelo virus and Black Friday virus have appeared continuously, which indirectly pushed forward computer security legislation at this stage.

As computer security issues successively arose in various places, local legislation also played a crucial role in the early stage of China's legal construction in cybersecurity. In September 1990, Heilongjiang Province People's Government released the Regulations on Security Management of Computer Information System in Heilongjiang Province (now invalid), pointing out that computer information system refers to the information processing system (including single-closed system) made up of computers as well as related and supporting equipment, facilities, information and staff. Computer system security refers to avoiding all types of unintentional errors and damages, preventing the computer system and data from being illegally exploited or destroyed, and guaranteeing the normal operation of the computer system. As a local government regulation, this provision offered practical experience for the setting of Decree No. 147.

1.1.2 Legislative Process

In February 1994, the State Council officially published the Regulations on the Protection of Computer Information System Security (Decree No. 147), which was China's first administrative regulation specially worked out for cybersecurity issues. In line with the State Council's guiding spirit that "the first regulation shall be coarse rather than fine principally and leave room for development and change", Decree No. 147 basically implemented the three strategic measures proposed by China in the early days, focusing on guaranteeing the security of computer information systems. First, it clarified the supervision mechanism. As the security issues arising from the popularization and application of computers are considered social problems, a supervision system has been set up for the heads of public security units, the Ministry of National Security, the National Administration of State Secrets Protection and other relevant departments of the State Council to do relevant work well within the scope of their duties. Moreover, ensure that there are laws to abide by. Clearly, define the concept of computer information systems and their security protection, specify the scope of application and crucial objects of security protection principally, set up and carry out a series of regulations such as security classified protection, international networking filing, sales licenses for special products, etc., and fulfill computer security supervision in accordance with the laws. Finally, punish illegal crimes. Decree No. 147 grants the Ministry of Public Security certain security supervision authority. I. Unify and standardize, supervise, inspect and guide the security protection of computer information systems; II. Investigate and deal with illegal and criminal cases that endanger the security of computer information systems; III. Perform other supervisory duties of security protection of computer information systems; IV. Inform the user unit to take security protection measures in a prompt manner when potential security hazards are found; V. Grant the Ministry of Public Security emergency

legislative power for specific matters, that is, special general orders, in a bid to leave the Ministry of Public Security with authority and lay a foundation for subsequent application with uncertainty.

Decree No. 147 defines a redline for national security protection and mandates that all units and individuals make use of computer information systems within the statutory security specifications. In brief, Decree No. 147 has three highlights. First, it incorporated cybersecurity into facility security for protection in the early 1990s, when the networking function was confined to a few areas and was not yet popularized. As the definition of a "computer information system" indicates, a computer serves as the main element, while the related and supporting equipment and facilities means the configuration of information system-related equipment, that is, the software and hardware required for the normal functioning of the system and the application of business data/information processing functions. The supporting facilities include computer room building, site environment, power supply, related communication equipment and lines inside and outside the system, etc. The reason why the network is included is that the basic functional characteristics of the network are interconnection and communication, and the network is an interrelated system made up of nodes and connecting lines, that is, the system. Computer systems and information systems chiefly composed of computing devices are characterized by interrelated operation, communication and resource sharing between their internal functions. If there is no correlation, the system and information are only isolated islands, and it is impossible to fulfill informatization and modernization. Thus, it is necessary to bring the network into the security of facilities for protection. In addition, it emphatically protects the security of computer information systems in crucial areas such as state affairs, economic construction, national defense construction, and cutting-edge science and technology. While drawing lessons from the relevant experience of crucial infrastructure legislation abroad, this article clarifies that the security of China's computer information systems emphasizes the safe and normal running of national functions, the smooth progress of economic construction and scientific and technological development, and national defense construction and defense security. Therefore, it is proposed to emphatically protect the security of computer information systems in crucial areas, among which economic construction covers a wide range, and Decree No. 147 is not exhaustive. Finally, with respect to security supervision, public security units are granted supervisory powers in security protection, investigation and punishment of illegal crimes, etc., which shows the determination of the state to strongly guarantee the operation of computer information systems as well as their associated networks and the order and security of virtual social activities in cyberspace, facilitate the application and development of computers, and guarantee the smooth progress of socialist modernization.

Specifically, Decree No. 147 has set up nine systems to guarantee the security of computer information systems, as follows:

1 Carry out legal and standardized security protection. Decree No. 147 requires that the construction and application of computer information systems shall be subjected to laws, administrative regulations and other relevant provisions of

the state. The system construction and maintenance party shall comply with and carry out relevant laws and regulations and relevant state regulations, do well in system security construction and security maintenance management, and violations of law must be investigation; those who engage in business applications and information processing with system resources shall comply with laws and regulations and relevant state regulations, and lawbreakers must be prosecuted. Legalization renders it necessary to transform the national laws, regulations and provisions on security protection into the security policy system of computer information systems as well as their associated networks and integrate the system of security control rules in the course of data/information calculation and processing in the system operation and application to ensure the automatic execution of computing equipment. Finally, for security protection, construct the overall security defense system of computer information systems as well as their associated networks, dominated by the system of rules of legalization of security policy and with the security control mechanism of computing process of computing environment as the focus.

2 Set up and implement the security classified protection system. Level, in essence, is a natural attribute, and the classification of levels is a benchmark scientific method for security protection. In the information age, all sorts of computer information systems and their associated networks in various areas of the country are vital strategic resources, and therefore, it is of significance to carry out scientific and reasonable security protection measures. From the point of reality, the construction of classified protection system is a necessary trend, and it is imperative to offer security classified protection for national computer information systems as well as their associated networks in line with the law and standards, and ensure the key points; construct a deep, multilevel and overall security defense system from small to large, from point to area and from inside to outside to enhance the security defense capability, dominated by the system of legal security policy and with the science of computing environment and safety control mechanism of computing process as the focus; carry out a classified protection system and build a five-in-one scientific protection system for the security and risk prevention of computing equipment, systems as well as their associated networks and virtual environment, which includes measurement (security level to be grasped in construction and management), assessment (self-assessment and evaluation), testing (self-testing and examination), supervision (industry supervision and law enforcement supervision) and investigation (self-investigation and law enforcement investigation), and enhance the capability of security protection. The classification of security protection levels chiefly considers the social and economic value level of system resources, the risk level of system resources facing hazards, the level of science and technology support capability of system security, and the level of security protection intensity that the country shall implement.

3 Establish the security protection system for computer rooms. Computer room, data center, etc. are the essentials of computer information systems, and hence

the security protection of infrastructure such as computer rooms of important computer information systems shall comply with relevant state regulations.

4 Construct the administration system of international networking filings. Upholding the concept that filing is a means and management is an end, Decree No. 147 specifies that the international networked computer information system shall comply with the relevant national and departmental regulations and standards on security protection and try to understand the international networking of computer information systems and the security protection of the access flow of data/information as much as possible.

5 Implement the custom transit declaration system of computer information media. The incoming/outgoing computer information media passing through the customs gate shall be declared to the customs, and the customs shall be responsible and entitled to inspect the incoming/outgoing computer information media.

6 Clarify the responsibility and institution of security management of computer information systems. The effectiveness of security protection work requires each unit's strict performance of duties, the perfection of the security management system and the formation of a system operation mechanism.

7 Carry out 24-h reporting system of cases. In the security management system of computer information systems, the responsibilities and procedures for case discovery, preliminary judgment, evidence retention, emergency response, and reporting shall be set up to cooperate with public security units to accept and investigate in a prompt manner and jointly safeguard the security of computer information systems.

8 Set up and optimize centralized management systems for the prevention and control of harmful data such as computer viruses. Harmful data, such as computer viruses, easily diffuse by virtue of the interconnection and immediacy of the network. To prevent proliferation or more harm, it is under the centralized management of the Ministry of Public Security.

9 Establish the sales license system of special products for security of computer information systems. To guarantee the security of computer information systems, the security concept shall be embodied throughout the life cycle of related equipment (products) from design to post maintenance. The security equipment (products) used to build security systems as well as their associated networks shall be guaranteed to conform to national standards and security regulations from the aspects of design scheme, production process, sales and use, aiming to strongly facilitate the autonomy and controllability of crucial information technologies through the sales license management system and government procurement system and to guarantee the security construction needs of computer information systems as well as their associated networks.

Furthermore, Decree No. 147 specifies that the measures for security protection for unconnected microcomputers shall be worked out separately. Since microcomputers include portable computing equipment, connecting it to computer information systems and their associated networks is terminal computing equipment, which is

controlled by a system security mechanism. Unconnected microcomputers cover a wide range of areas, undergoing enormous changes and facing complicated situations. It is not suitable for the national legal level to offer a unified method for security protection. Decree No. 147 shall be worked out separately, which means that various industries, departments, units and institutions can draw up reasonable measures for security protection in consideration of the actual circumstances and needs and with reference to relevant regulations.

Generally, the promulgation and enforcement of Decree No. 147 has made zero breakthroughs in China's legislation of information security, filled the gap of legal norms in the information age, and laid a solid foundation for supporting systems and local legislation. Upon promulgation of Decree No. 147, the revision of the Criminal Law of the People's Republic of China (hereinafter referred to as Criminal Law), the People's Police Law of the People's Republic of China (hereinafter referred to as the People's Police Law), the Law of the People's Republic of China on Penalties for Administration of Public Security (hereinafter referred to as Law on Penalties for Administration of Public Security), the setting and revision of departmental regulations, local regulations, relevant military regulations and relevant national information security protection standards have gradually started.

With respect to the security classified protection system, in September 1999, the Ministry of Public Security organized the drafting, and the State Bureau of Technical Supervision published the first mandatory national standard for information security protection in China—Classified Criteria for Security Protection of Computer Information Systems (GB17859-1999). This standard also adopts the method in the principle of being coarse rather than fine, which is intended to offer technical guidance and foundation for the development of security products, the setting of specific standards, the construction and management of security systems, relevant laws and regulations and their enforcement. The standard classifies the security protection capability of computer systems into five levels, namely, user independent protection (Level 1), system audit protection (Level 2), security mark protection (Level 3), structured protection (Level 4), and access verification protection (Level 5). Along with the increase in security level, computer information systems have become increasingly capable of security protection.

In April 1994, China officially accessed the Internet. To ensure that international networking has rules to follow and laws to abide by, in February 1996, the State Council released the Interim Regulations of the People's Republic of China on the Administration of International Networking of Computer Information Networks (Decree No. 195) from the point of view of reinforcing industry management, requiring computer information networks to directly connect with international networks and use the international entrance and exit channels furnished by the national public telecommunication network of the Ministry of Posts and Telecommunications. No unit or individual may set up itself or connect with international networks through other channels. License management should be employed for the business activities to be working on, and the examination and approval system should be applied to the nonbusiness activities. Apart from that, providers of international

entrance and exit channels, interconnection units and access units shall set up corresponding network management centers, reinforce the management of their own units as well as their users, and do well in security management of network information. Units and individuals working on international networking business shall strictly execute the security and confidentiality system and shall not launch illegal and criminal activities such as endangering national security and revealing state secrets by taking advantage of international networking. Based on Decree No. 195, the Ministry of Posts and Telecommunications and the State Education Commission successively promulgated the Measures for the Administration of International Networking of Public Computer Internet in China and the Interim Measures for the Administration of Education and Research Computer Network in China in the same year, respectively, to reinforce the management of international networking of public computer Internet and education and research computer network (CERNET).

The computer security problems faced by our country are not limited to the computer system security level by accessing the international network. To address the new problems endangering social security, such as the influx of illegal and harmful information incurred by the international networking of computers, in December 1997, the Ministry of Public Security released the Measures for the Administration of Security Protection for International Connections to Computer Information Networks (Decree No. 33 of the Ministry of Public Security) for the sake of guaranteeing the security of international networking of computers. Decree No. 33 of the Ministry of Public Security is based on the higher-level laws of Decree No. 147 and Decree No. 195, which specify that the computer management and supervision institution of the Ministry of Public Security shall be responsible for the security protection and management of international connections to computer information networks; Units and individuals working on international networking business shall accept the security supervision, testing and guidance of public security unit, truthfully furnish public security unit with information, materials and data associated with security protection, and offer assistance for public security unit to investigate and deal with illegal and criminal acts through computer information networks connected to the international network. Decree No. 33 also specifies five types of harmful behaviors of computer information cybersecurity that are prohibited, including accessing computer information networks or making use of computer information network resources without permission; deleting, modifying or adding functions of computer information networks; deleting, modifying or adding data and applications stored, processed or transmitted in the computer information network; and deliberately making and spreading destructive programs such as computer viruses, which endanger the security of computer information networks.

Additionally, to cope with the inflow of a large amount of false and harmful network information after international networking, Decree No. 195 and Decree No. 33 of the Ministry of Public Security have clearly come up with the management of network information content. Decree No. 195 requires that information that hinders public order and contains obscene pornography shall not be produced, consulted, copied and disseminated; Decree No. 33 of the Ministry of Public Security prohibits the production, reproduction, consultation and dissemination of nine