Article

Comparative study on criminal legislation of cyber crime between China and Japan

Tang Ming

[1] Sichuan Agricultural University; 154097164@qq.com
* Correspondence: Tel.: +86 16602821388

Abstract: Cyber crime is a problem that China and other countries all over the world are facing. In order to deal with this problem, various countries have formulated different measures in the field of criminal law, and Japan is one of the typical representatives of the developed countries with the rule of law in the world. Therefore, this study compares and analyzes the characteristics of cyber crime legislation in China and Japan, and uses it for reference to make up for the shortcomings of our country, so as to better curb cyber crime.

Keywords: China; Japan; cybercrime; criminal legislation

Academic Editor: Wuyu WO

Received: August 1, 2025
Revised: NA
Accepted: August 3, 2025
Published: August 16, 2025

1. Introduction

The rapid development of information and communication technology and digital computing equipment has brought convenience to people's daily life and communication. According to the survey of the China Internet Information Center, as of June 2015, more than half of China's residents were using the Internet, including more than 600million people using the Internet to communicate with others, more than 500million people using the Internet to search for news, and more than 400million people using the Internet to make online shopping. The survey also shows that other online services, such as personal blogs, online videos and online games, also have a large number of users [1].

While network technology has brought convenience to people's lives, it has also contributed to the arrogance of cybercrime. In recent years, with the rapid development of network technology, China's network crime rate remains high, and the forms of network crime are gradually diversified, which has brought great challenges to China's fight against network crime, and the crime situation is not optimistic. However, the current legislation against cybercrime in China is not perfect, and Japan, as one of the countries with developed rule of law in the world, has advanced experience in cybercrime legislation. Therefore, through the comparative analysis of the characteristics and legislation of cybercrime in China and Japan, this paper finds the shortcomings of the existing legislation against cybercrime in China, and uses the advanced experience of Japan for reference, so as to better curb the development of cybercrime in China.

2. Comparison of characteristics of Chinese and Japanese cyber crimes

2.1 Characteristics of Cybercrime in China

With the continuous advancement of internet technology, China's cybercrime landscape remains alarming, characterized by extensive scope and staggering financial losses. According to a Norton Security Report released by Symantec in November 2012,

global individual users suffered massive cybercrime losses totaling $110 billion between July 2011 and July 2012. In China alone, 260 million people were affected by cybercrimes, resulting in economic losses of 289 billion yuan [2]. In 2012, through coordinated efforts by Chinese public security authorities, approximately 118,000 cybercrime cases were cracked, with 216,000 suspects apprehended and 340,000 illegal websites shut down [3]. These figures demonstrate the escalating severity of cybercrime, posing significant challenges for China's law enforcement in protecting citizens' legal rights. Concurrently, statistics from the China Internet Illegal Information Reporting Center reveal a steady rise in citizen reporting of illegal online activities, indicating both worsening cybercrime trends and growing public awareness. Current analysis identifies major cybercrimes with severe societal impact and wide-ranging effects in China: online fraud, pornography, copyright infringement, gambling, and computer viruses.

In conclusion, cybercrime currently poses significant challenges to China. Faced with this challenge, public security authorities cannot afford to relax their efforts, as combating cybercrime remains a long-term task. Based on the above information, the characteristics of cybercrime in China can be summarized as follows:

First, cybercrime perpetrators are increasingly becoming younger. Data from recent years shows that most current cybercriminals are young adults, with an alarming trend of participants getting younger, including minors. According to Hubei Province's investigation reports on cybercrimes, over 90% of offenders in 2012 were under 30 years old. This is mainly due to the decreasing barriers to entry for cybercrime. With advanced information networks, criminal activities can be easily found and replicated online. Young people often lack legal awareness and self-discipline, making them particularly prone to committing crimes through digital platforms. Consequently, a significant portion of cybercrime perpetrators now concentrate among adolescents.

Secondly, cybercrime is evolving into an industrialized operation. As cybercrimes continue to develop, they have transitioned from sporadic incidents to organized criminal activities conducted by specialized teams with clear division of labor. Analysis of a common online account theft case reveals that perpetrators exhibit distinct phases and specific roles: programming attacks, creating botnets, exploiting network vulnerabilities, and launching website assaults. These specialized divisions mirror different industrial sectors. The resulting industrialized cybercrime chain further enhances operational professionalism. This professionalization not only boosts efficiency but also spreads risks, ultimately causing greater harm to Chinese society and citizens.

Third, the diversification of criminal tactics has intensified. As time progresses and public awareness of cybercrime prevention grows through targeted campaigns, coupled with increasingly stringent crackdowns by law enforcement agencies, cybercriminals have adopted innovative methods to infiltrate every corner of society. Their evolving modus operandi leaves netizens defenseless against these sophisticated schemes, ultimately trapping them in elaborate criminal traps.

2.2 Characteristics of Japanese cyber crime

Japan has also been plagued by cybercrime. According to the 2012 Cybercrime Report and Advisory Report, the country recorded approximately 7,330 cybercrime cases in 2012, marking a 1,600-case increase (27.7% growth) from the previous year and reaching a historic peak [4]. Analysis of Japanese cybercrime cases reveals the following key characteristics:

First, using the Internet to commit fraud is a crime with high crime rate. It not only maintains the largest proportion, but also changes its criminal mode. Fraud has always been a kind of crime with bad influence and great impact in Japanese society.

Second, the rapid increase of crimes committed by minors. The main reasons are that minors have a weak ability to distinguish right from wrong and are easy to be targeted by criminals. In addition, the popularity of smart phones connects criminals with minors, and a large number of bad information can easily spread among minors.

Third, the young age of the criminal subject. According to the data provided in the "Report on the Reporting and Consulting of Cyber Crimes in 2012" by the Japan Police Agency, more than 40% of the reported cases were committed by people around the age of 10. Therefore, it can be seen that the problem of the young age of cyber crime subjects in Japan is more serious than that in China [5].

2.3 Content comparison

The analysis reveals that while Chinese and Japanese cybercrimes share significant similarities, they each exhibit distinct characteristics. The trend toward younger perpetrators is particularly pronounced in Japan. Although China's current data shows less severe issues compared to Japan's, the problem remains concerning. Moreover, both countries are increasingly witnessing professionalization and scaling of cybercrime activities. This not only presents challenges for their respective nations but also poses a global threat to cybersecurity, demanding strengthened international cooperation to address these challenges collectively.

3. Comparison of criminal legislation between China and Japan

3.1 Overview of Legislation in China

Up to now, China's legislation on cyber crime can be roughly divided into the following three stages: opening legislation, formal legislation and the revision and improvement of criminal law.

The first phase initiated legislation. China's computer-related legislation marked the beginning of its cybercrime governance framework. In 1983, the Ministry of Public Security established the Computer Management and Supervision Bureau with clearly defined responsibilities, designating it as the primary authority for national computer security [6]. The drafting of China's "Regulations on Computer Information System Security Protection" in 1988, which came into effect in 1994, marked a new starting point for cybersecurity and cybercrime prevention efforts. However, since internet usage was not yet widespread in China at the time, these regulations primarily focused on computer security protection rather than encompassing network security measures.

The second phase involved formal legislation. As cybercrime cases in China continued to escalate over time, causing severe violations of citizens 'rights, they garnered significant attention from both legislators and the public. To address this challenge, Chinese lawmakers, building on accumulated case studies and incorporating expert recommendations, introduced the crimes of unauthorized access to computer information systems and destruction of such systems during the 1997 Criminal Law revision. The amendment also established provisions for financial fraud, theft, embezzlement, misappropriation of public funds, and other cybercrimes committed through computers, which would be prosecuted under relevant criminal law provisions [7]. This timely revision demonstrates that the Criminal Law's updates have effectively curbed the spread of cybercrime to some extent.

The third phase focused on legislative refinement. When China revised its Criminal Law in 1997, the emphasis was placed on protecting computer information systems for state affairs, national defense, and high-tech sectors, while neglecting commercial and personal data protection. To address this oversight, the Criminal Law underwent another amendment in 2009. The updated provisions expanded information protection

from these three key areas to include commercial and personal domains, effectively addressing shortcomings of the initial phase. This comprehensive overhaul significantly safeguards individual rights and maintains social stability.

3.2 Legislative Overview of Japan

The legislation of cyber crime in Japan can also be divided into three periods: the stage of criminal law amendment in 1987, the stage of enactment and modification of the Law on Prohibition of Illegal Connection, and the stage of partial amendment of criminal law in 2011 [9].

The first period was the revision period of criminal law. Japan revised the criminal law in 1987 and made it a part of the criminal law, but the focus of the revision of the criminal law was on the punishment of existing computer crimes in the past, rather than supplementing new network crimes. Therefore, there was no substantive change in the criminal law at this stage.

The second phase involved the enactment and amendment of the wiretapping prohibition law. When Japan revised its Criminal Code in 1997, the lack of substantive amendments significantly conflicted with U.S. information security interests at the time. Under intense American pressure, Japan was compelled to revise regulations governing unauthorized access to computers. Subsequent revisions established two key components: first, penalty guidelines for violations; second, protective measures requiring telecommunications operators to implement safeguards. Telegraph operators could request assistance from prefectural or state authorities and other defensive strategies.

The third phase focused on revising and refining the Criminal Law. In 2011, Japan amended its Anti-Unlawful Connection Prohibition Act, introducing a new chapter on crimes involving improper electromagnetic recording. To combat the production, supply, and acquisition of computer viruses, two specific offenses were added under the Chapter on Crimes of Improper Directive Electromagnetic Recording: —— Crime of Improper Directive Electromagnetic Recording Production and Crime of Improper Directive Electromagnetic Recording Acquisition.

3.3 Comparison of criminal legislation of the two countries

3.3.1 Content comparison

Initially, when revising cyber legislation, Japan failed to recognize that cybercrime had begun infringing upon citizens 'new rights. Consequently, it merely supplemented and refined existing laws without introducing new provisions. Later, under U.S. coercion, Japan was compelled to enact the Prohibition of Misconduct in Cyberspace Act. This legislation introduced flexibility in criminal policy during its formulation, significantly enriching Japan's legal framework [10]. The 2011 and 2012 amendments to relevant laws truly ushered in a new era of cyber protection. In summary, from a content perspective, Japan's cybercrime legislation has undergone a continuous evolution—from prioritizing traditional legal interests to addressing emerging ones. Therefore, Japan's cyber legislation demonstrates advanced approaches in regulating both traditional and modern legal interests.

3.3.2 Formal comparison

Japan's legislation against cybercrime encompasses nine criminal offenses and a specific Act Prohibiting Unauthorized Access. This act primarily addresses penalties for hacking intrusions. The prohibition of unauthorized access refers to illegal computer intrusions and actions compromising information security, while the crimes of destroying private and public documents involve tampering with the integrity and accessibility of computer data. Although the crime of damaging electronic systems

appears to infringe upon the integrity and usability of computer systems, it actually involves not merely damaging computer infrastructure but rather using such acts as means to disrupt others' normal operations [11]. In summary, offenses like improper creation and provision of electromagnetic records, forgery of original notarized documents, use of forged credentials, and computer fraud should be categorized as computer-related offenses. Meanwhile, the crimes of creating electromagnetic records, obtaining such records through unauthorized means, and the "pre-intrusion conduct" under the prohibition of illegal access actually regulate preparatory acts assisting or facilitating unlawful intrusions. This analysis demonstrates that Japan's current cybercrime legislation, while appearing comprehensive in form, effectively adapts to the complex challenges posed by modern digital threats.

3.3.3 Comparison of specific charges

China's current criminal law imposes broader penalties for cybercrimes compared to Japan, yet its implementation lacks practicality in practice, failing to achieve the goals of preventing and combating such offenses. In contrast, Japan's cyber legislation has evolved through continuous exploration and breakthroughs. It not only established independent charges for traditional computer-related crimes but also provided judicial authorities with legal grounds to combat computer forgery and fraud. Building on this foundation, Japan has continuously revised and improved its cybercrime legislation [12]. Therefore, Japan's experience demonstrates that different types of cybercrimes should be treated differently to better implement the principle of legality in criminal law.

In conclusion, through comparative analysis of legislation between China and Japan, it is evident that China's cybercrime legislation exhibits certain deficiencies in content. Although subsequent revisions have been made, these primarily involved adding clauses without systematic logical justification. Therefore, by drawing on Japan's advanced legislative practices in cybercrime, we should address the shortcomings of China's current legislation to more effectively curb cybercrimes.

4. Implications of the comparison between Chinese and Japanese criminal regulations on cyber crime

4.1 Formulate special criminal law

The landscape of cybercrime is constantly evolving, with criminals expanding their reach into every corner. Relying solely on a few provisions in existing criminal law proves insufficient to combat these digital threats. Given the current characteristics of cybercrimes in China, it has become imperative to enact specialized legislation to address this challenge. Moreover, the increasing professionalization and industrialization of cybercrime indicate that traditional criminal law alone cannot effectively tackle these complex issues. We must develop more scientific, detailed, and specialized legal frameworks to eliminate cybercrime's breeding ground [13]. Therefore, establishing dedicated laws to combat cybercrime has become both necessary and urgent in this rapidly changing digital environment.

4.2 Lower the age of criminal responsibility for cyber crimes

The increasing prevalence of young offenders in cybercrime makes lowering the age of criminal responsibility for such offenses imperative. Without policy adjustments, today's severe cybercrime landscape will not only fail to be contained but may escalate [14]. Given teenagers' strong curiosity and lack of legal constraints, their potential harm to society could prove incalculable. Therefore, appropriately lowering the age of criminal responsibility for cybercrimes is crucial to regulate this vulnerable group.

4.3 Strengthen international cooperation in combating cyber crimes

The transnational and cross-regional nature of cybercrime has created a significant challenge for China and the global community. This situation makes it imperative to strengthen international cooperation in addressing this issue. First, China should actively collaborate with international organizations while adhering to its own cybercrime prevention requirements, further fulfilling and implementing relevant international obligations and rights. Second, it is crucial to expand cooperation and exchanges with advanced nations worldwide, learn from their proven strategies in combating cybercrime, address domestic shortcomings, actively seek international collaboration opportunities, and enhance judicial assistance mechanisms in cybercrime investigations [14].

5. Conclusions

In summary, Japan's current legislation against cybercrime demonstrates superior legislative techniques in both protecting traditional legal interests and emerging legal interests compared to China. Therefore, China should actively learn from and adopt Japan's advanced practices. As modern networks experience explosive growth and rapid proliferation, cybercrime has become a global concern. By integrating international criminal law systems on cybercrime, China can absorb legislative experiences and identify gaps to continuously improve its cybercrime legislation. This will enable more comprehensive prevention and crackdowns on cybercrimes, thereby stabilizing the nation's socio-economic development order and safeguarding citizens' personal and property rights. Through analyzing, comparing, and proposing improvements to China's cybercrime criminal system, we aim to contribute to the refinement of China's cybercrime legislation.

References

1. Chen Qinfa. Analysis on Network Crime Governance in China under the Background of Big Data [J]. Journal of Hubei University of Science and Technology, 2020(2):48-52.
2. Liu Wenyan and Yan Jian. Research on Computer Network Crime in the Perspective of Criminal Law [J]. Journal of Shaanxi Administrative College, 2020,034(002):101-104.
3. Wang Haijun. On Cybercrime from the Perspective of Criminal Law [J]. Journal of Economic Research, 2018,000(018):198-199.
4. Li Ming. Key Countermeasures and Implications of Preventing Computer Cybercrime in Japan [J]. Journal of Guangzhou Public Security Management Cadre Institute, 2012(02):18-21.
5. Cao Ya Wen. Legal Countermeasures and Reference for Japan's Governance of Cybercrime [J]. Journal of the People's Public Security University of China (Social Sciences Edition), 2018,34(02):130-138.
6. Jiao Yang. Research on the Criminal Law Regulation of Cybercrime [D]. Inner Mongolia University, 2017.
7. Sun Yeli and Jin Lai. Discussion on the Criminal Law Regulation of Cybercrime [J]. Legal Expo, 2018(10):146-147.
8. Zhong Chongyi. Research on the Legal Restriction Dilemma and Countermeasures of Cybercrime in China [J]. Legal Expo, 2020(33).
9. Qi Aimin and Liu Ying. Research on Internet Law [M]. Beijing: Legal Publishing House, 2003.
10. Wu Dahua. Research on Criminal Rule of Law [M]. Beijing: People's Public Security University Press, 2012.
11. Zhang Chao. Japan: A Multi-pronged Approach to Internet Regulation [J]. Citizen and Rule of Law, 2013(2):48-49.
12. Wu Guijing. Comparative Study on Criminal Legislation of Cybercrime in Various Countries [J]. Economic and Law, 2003,000(003):28-29.
13. Wang Guangkun. On the Improvement of Cybercrime and Criminal Legislation in China [D]. China University of Political Science and Law, 2017.
14. Xu Yali. Research on International Criminal Judicial Assistance in Cross-border Cybercrime [D]. Nanchang University, 2020.