Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231216

Intrusion into Computer Information System: Criminal Law Rule Based on Different Judicial Recognition Perspectives of State Affairs

Yinuo Liu[1,a,*]

[1]*College of Criminology, People's Public Security University of China, Beijing, 100091, China*
a. Dao.sprefe@natains.org
**corresponding author*

Abstract: Cybercrime refers to a new form of crime generated with the application and prevalence of computer technology. In China, there are increasingly more instances of unauthorized access to computer systems every year, which has severely affected network security and the property security of the people, and even national security. This paper delves deeper and more methodically into the problems surrounding the criminal act of unlawful access to computer information systems. The ambiguous definition and limited reach of the criminal object make China's punishment for unauthorised access to computer systems less effective., the crossover of the criminal law system caused by the contradiction of legislative logic, as well as the insufficient prevention of too lenient penalties. Based on the above legislative deficiencies, it is imperative to improve the criminal law system, expand the protection scope of the first clause of Article 285 of the Criminal Law, Increase the number of cases that are investigated and prosecuted, explain computer information systems in the context of state affairs, expand the definition of "state affairs" computer information systems, and strictly regulate the amount of crime that is legal. Additionally, it is essential to establish an independent status for data crimes by adding provisions on data security protection concerning the three major computer information systems; increasing the intensity of punishment, raising the range of statutory penalties, and adding property penalties, thereby imposing a comprehensive regulation on illegal intrusion into computer information systems.

Keywords: cybercrime, state affairs, computer information system, legislative improvement

1. Introduction

According to the statistical data analysis of the national network security department, from 2017 to 2021, Chinese courts at all levels resolved more than 282,000 cases involving information network crimes, with the incidence of cases not declining but merely increasing, and the majority of the intrusions coming from outside of China. Due to the severity of the issue, it is imperative that China's computer networks and information systems are better protected and secure. The best way to enable the speed of legislative improvement to adapt to the fast development of computer technology has emerged as a critical issue confronting the current Chinese criminal law to better ensure the security of the relevant computer information system. Due to the severity of the issue, it

DOI: 10.54254/2753-7048/17/20231216

is imperative that China's computer network information systems must be better protected and security enhanced. The best way to enable the speed of legislative improvement to adapt to the rapid growth of computer technology has emerged as a critical issue confronting the current Chinese criminal law in order to better ensure the security of the relevant computer information system. If the suppression is not effective, the security of the computer information system in the crucial areas covered by this crime will be seriously threatened. Under this trend, countries around the world have also intensified their legislative efforts to crack down on such crimes, such as Germany, which has established data security crimes to crack down on this, and the United States, which has also included such crimes in computer crimes to crack down on them. China, as a developing country, took a late start in this area, while also attaching great importance to it. As early as 1997, The current Article 285 of the Criminal Law was amended in 2009 by the Seventh Amendment to the Criminal Law, which added this crime to the list of crimes covered by the provisions of the Criminal Law in Chinese law. All of these are punishable under Article 285 by a fixed-term prison sentence of up to three years or detention, including illegal interference with state affairs, national defense initiatives, and cutting-edge scientific and technological areas of computer information systems. (Illegal control of the computer information system and illegal acquisition of computer information system data are both against state law.)

Unauthorized entry into the computer information system will result in a fixed-term prison sentence of up to three years or detention with a fine or a single fine, depending on the severity of the circumstances, the use of other technical methods to access data that has been stored, processed, or transmitted in a computer information system or to gain unauthorized control over one. Provide programs or tools specifically for illegal access to or control of computer information systems, or with knowledge of the gravity of the offense, provide programs or tools for others to do so; both actions are punishable in accordance with the aforementioned provisions. If the organization commits the first three offenses, it will be fined and its directly responsible managers and other directly responsible individuals will be subject to the provisions of the relevant laws. Since this revision, several experts and scholars in the Chinese criminal law profession have also studied crime more intensively, new issues have continuously emerged, with different views on the identification of state affairs in the academic community. For instance, the Interpretation of Crimes Against Computer Information System Security had taken into consideration the weakening of the concept of "state affairs" to "state organs" during the drafting process. Afterward, the Interpretation proposed to stipulate with the comprehensive views of the academic community that computer information systems involving security and interests in the fields of politics, economy, national defense, foreign affairs, and social management should be recognized as computer information systems in the three important fields of state affairs, building national defense, and cutting-edge science and technology (hereinafter referred to as the three important computer information systems). These three key computer information systems tended to broaden the judicial recognition of state affairs at this time. Thereafter, some scholars suggested that, in view of the mutually exclusive nature of the first and second clauses of Article 285 of the Criminal Law, the first clause merely provides for the objective element of "intrusion", without a clear definition of "state affairs, national defense construction, and cutting-edge science and technology" to limit its application, the crime of unauthorized intrusion into computer information systems should be used only "sparingly and cautiously", to make sure that there is legislation for the protection of significant computer information systems and that additional suitable provisions can be found in the Criminal Law in the event that additional criminal acts occur after illegal infiltration into computer information systems in the three main fields [1]. As of now, the evaluation basis adopted for state affairs is the Interpretation of Crimes against Computer Information System Security promulgated by the two high authorities on 1 August 2011, in which Article 10 makes a procedural provision for

DOI: 10.54254/2753-7048/17/20231216

determining “state affairs”, “entrusting the department responsible for computer information system security and protection management above the provincial level”, the final recognition is made by the judicial organs. Since there has been no relevant judicial interpretation of “state affairs” to clarify, leading to a unified perception in judicial practice. As a consequence, from a general point of view, it is of great practical significance to conduct an in-depth discussion on the existing issues in the application of this crime in practice and the improvement of legislation. On the basis of comparing the relevant legal systems of other countries, In order to look into the issues related to legal improvement and the crime of illegal access to computer information systems in China, this paper uses the current issues of the law’s application to such crimes in legislation and judicial practice.

2. The Main Practical Difficulties

2.1. The Contradiction of Legislative Logic Leads to Unbalanced Crime and Punishment

The misuse of data, which is an implicated crime, is what the culprit wishes to pursue; the unauthorized entry into the computer information system is just a means to that end. However, due to the dearth of criminal law legislation in China, this may result in the use of the crime of unauthorized entry into computer information systems to be regulated, which cannot implement the fundamental principle of adapting criminal law to crime and punishment. The author attempted to compare the first clause of Article 285 (the crime of illegal intrusion into computer information systems)with the second clause of Article 285 (the crime of illegal access to computer information system data, illegal control of computer information systems)for analysis: if the perpetrator illegally invaded the three major computer information systems to further obtain data and information that does not fall under the state secrets, commercial secrets, the crime cannot be absorbed by the crime of illegal access to state secrets, intelligence crimes, and espionage.

However, because the goal of the crimes of unauthorized access to computer data and unauthorized control of computer systems is the exact reverse of the earlier offense, they cannot be covered by this section, which can only be sentenced to less than three years of imprisonment in accordance with the first clause of Article 285 of the Amendment to the Criminal Law of the People’s Republic of China (XI) adopted on December 26, 2020. In contrast, the sentence for a conviction under the second clause of Article 285 of the Criminal Law is imprisonment or detention for a term of up to three years and a fine or a single fine if the circumstances are “serious”; if the circumstances are “particularly serious”, Sentenced to a term of imprisonment of not less than three years and not more than seven years and fined. To put it in another way, if the three major computer information systems that should have been protected in focus were to reach the particularly serious acts stipulated in the second clause of Article 285 of the Interpretation of Crimes against the Computer Information System Security, which came into force on 1 September 2011, the sentences would be lighter than those for the same criminal acts committed by intruding into general computer information systems. From the perspective of legal benefit infringement, illegal access to computer information system data in the areas of national affairs, national defense planning, and cutting-edge science and technology is significantly worse than that of illegal intrusion into the computer information system [2]. It goes against the original legislative aim of the felony of unauthorised entry into a computer information system. For instance, in the case of illegal intrusion into the official website of Traffic Control 12123, Dai used illegal means to log in and obtain the license plate information on the website of Traffic Control 12123 and helped others to check the number on the license plate for a profit of RMB 78,500. Traffic Control 12123 is a mobile client-side application software provided by the Chinese Internet traffic safety comprehensive service management platform, technical support by the Chinese Ministry of Public Security Traffic

DOI: 10.54254/2753-7048/17/20231216

Management Research Institute, the application software provides drivers with a comprehensive, multi-level business processing and traffic safety services for motor vehicles, driver's licenses, and violations. Eventually, the court determined that "Traffic Control 12123" is a computer information system of state affairs, and defendant Dai was found guilty of illegally entering the system and given a nine-month prison term. On the other hand, in the case of the illegal acquisition of computer information system data of Company A by Sun, Sun broke through the verification by technical means and obtained a large amount of information data stored in the server of Company A, and offered it to others for profit, resulting in the company spending RMB 14,859.44 in response to the attack. The defendant Sun was ultimately found guilty of unauthorized access to computer information system data by the court, and he was given a one year and ten month prison term as well as an RMB 50,000 fine. In the case of Dai, by the Article 3 of the Interpretation of Crimes against Computer Information System Security issued by the Supreme People's Court and the Supreme People's Procuratorate of the People's Republic of China, the illegal proceeds of Dai reached the "particularly serious" circumstances of the crime of illegal access to computer information system data and illegal control of computer information system, which is punishable by a fixed-term sentence of imprisonment lasting more than three years but less than seven years, as well as a fine; while the case of Sun is far less serious than the case of Dai, both in terms of the level of the computer information system as the object of the crime, and the amount involved, whereas there exists a large difference in the final conviction and sentence. The objective behavior of the two crimes is different, a conduct crime is the unauthorized access to a computer information system, in comparison with the crime of the results of the second clause of Article 285 of the Criminal Law, which means that "serious consequences" must be achieved to constitute a crime. The designation of "intrusion" as this crime was meant to emphasize how the three main computer information systems are protected by criminal law by reducing the standard of proof, which deserve more comprehensive legal protection, the crime before and after the two clauses have appeared logically contradictory, with a certain degree of regulatory crossover in the legislation.

The Scope of the Crime Object is Too Narrow, Lacking an Explicit Definition of "State Affairs"

The unclear identification of "state affairs" has led to the fact that when determining computer information systems in related fields in judicial practice, the verdict tends to depend on the discretion of judges, resulting in various decisions being made in the same case. The theory of computer information systems in important areas like national affairs, economic construction, national defense construction, and cutting-edge science and technology as critical maintenance objects, based on the general provisions of the "Computer Information System Security Protection Regulations", some scholars have suggested that the interpretation concept of "state affairs" should be limited given the current state of judicial practice; In the process of the proposed provisions of the Interpretation of Crimes against Computer Information System Security, which came into effect on 1 September 2011, the major legal benefit of "economic construction" was ultimately chosen to be deleted, which represents that the crime demonstrated significant restraint in the legislation, while this crime should be treated as a backup provision and adopted the principle of "sparing and cautious use" as much as possible [1]. This perspective is reflected in cases involving computer information systems owned by state organs. For instance, in the case of the illegal solicitation of vehicle traffic violation business by Zhang, Zhang used illegal technical means to register on the "Traffic Control 12123" platform, in which he tampered with the phone numbers of drivers stored on the platform and bound the information of illegal vehicles, thereby resulting in the theft of points from the driver's license of the drivers. In this case, the prosecuting authorities believed that "Traffic Control 12123" is the official client-side of the Internet traffic safety comprehensive service management platform, which provides traffic management services for car owners and drivers nationwide, making the system a computer information system of the state affairs. In the

DOI: 10.54254/2753-7048/17/20231216

case of the alleged illegal intrusion into the public security traffic management comprehensive application platform, Gao in Ningde Public Security Bureau Traffic Police Detachment brigade served as a police officer during the off-duty time, he took advantage of the application platform to give a record of 206 violations of the Xie provided no penalty points for processing. Xie charged the drivers or owners of vehicles in violation of the law from RMB 50 to 80 per point while paying the suspect Gao a total of more than RMB 8,000. The court decided that the above-mentioned behavior of the suspect Gao was cause for suspicion of the crime of causing computer information system damage in this case rather than focusing the investigation on illegal entry into the "state affairs" computer information system. After the court reviewed and twice returned for additional investigation, where it was found that the evidence of the amount of illegal income was insufficient and did not meet the conditions for prosecution, it was determined that Gao was not prosecuted. The author considers that this case is attributable to the failure of the court to include the comprehensive application platform for public security traffic management into the scope of the "state affairs" computer information system to investigate and obtain evidence in the wrong direction, which ultimately led to its failure to punish violations of the law effectively. For this reason, the author takes an opposing view to the perspective of restriction. If in the aforesaid case, the intrusion into the state affairs system was merely for personal convenience, while further violations were committed to obtain data not involving significant confidential information, it would not be possible to rely on the first clause of Article 285 of the Criminal Law, if it is considered that the information platform of the local public security system should not be interpreted to apply to the state affairs in the crime of "illegal intrusion into computer information system" [2]. If the amount of illegally obtained data or the amount involved in the case does not reach the "serious circumstances" stipulated in the first article of the Interpretation of Crimes against Computer Information System Security, it will result in the inapplicability of the "crime of illegal control of computer information system" stipulated in the second clause of Article 285; if it cannot reach the "serious consequences" stipulated in the fourth clause of the above interpretation, it will not apply to the crime of damaging computer information system stipulated in Article 286 of the Criminal Law, which will, in turn, render such socially harmful acts incapable of being regulated by effective criminal law.

2.2. The Statutory Sentence Is Excessively Minor

The lenient convictions and sentences for cybercrime are likely to directly lead to the spread of cybercrime dynamics in the context of this information technology era, while also not conducive to the exercise of criminal jurisdiction in China. In accordance with the data in the big data special report on cybercrime judiciary released by the Supreme People's Court of China, a total of more than 282,000 cybercrime cases involving more than courts at all levels nationwide conclude first instance cases for 660,000 defendants from 2017 to 2021, with a year-on-year increase reaching 104.56% from 2021 to 2022, and the caseload remains on a year-on-year rise. The crime of illegal intrusion into the computer information system is a crime stipulated in the Chinese criminal law in 1997, through the case search of the author in the platform of the Magic Weapon of Peking University (regulation search database), revealed that among the relevant cases over the past ten years, there were 59 trials from 2013 to 2017 and 89 trials from 2018 to 2022, with an increase of 66% year-on-year, which indicates that the current conviction and sentence for the crime of illegal intrusion into the computer information system still does not meet the current need to effectively combat cybercrime [3]. Since cybercrime is characterized by the simplicity and intelligence of criminal methods, flexibility and industrialization of crime forms, it is extremely easy to organize multiple places and people to commit criminal acts against multiple groups through the Internet, which means that its legal interests are infringed widely in scope and to a high degree [4]. If the criminal law conviction of cybercrime fails to intervene in the preparatory stage of criminal

DOI: 10.54254/2753-7048/17/20231216

behavior through effective deterrence, it may result in the swift spread of cybercrime, which is not conducive to the protection of computer network security and the strict punishment of illegal acts of intrusion into computer information systems. Meanwhile, it may also lead to impeding the governance of criminal jurisdiction issues of cross-border illegal intrusion into computer information systems. Over recent years, the number of hacks on Chinese government computer information systems has increased, many of which have IPs originating from outside of China. In accordance with the current principle of protection jurisdiction under Chinese criminal law, the state only extradites suspects who commit crimes that may be punishable by more than three years in prison, while the maximum sentence for this crime is three years, which is also inherently detrimental to the deterrence of attacks on the three major computer information systems in China from abroad.

3. Causes of the Criminal Law System Issue of the Crime of Illegal Intrusion into Computer Information System

After China gained connection to the global Internet in 1994, with the use of computers becoming more widespread, hacking, virus propagation, system attacks, and functional damage committed against computer information systems have progressively emerged. In particular, hacking acts and computer sabotage against cutting-edge technology fields, government affairs, and large-scale portals have become increasingly rampant.

In response to the aforementioned constantly emerging illegal behavior and crimes endangering network security, Articles 285 and 286 of the Criminal Law, which deal with illegal intrusion into computer information systems and computer information system damage, respectively, were added to the Criminal Code that China adopted in 1997. These two new crimes are specifically designed to jeopardize the security of computer information systems. As a substantive law with language and writing as the carrier, Chinese criminal law inevitably features the inherent limitations of statutory law, which is specifically manifested as purposelessness, inconsistency, ambiguity, and lagging; in the creation of criminal law provisions for computer system crimes, the inconsistency of statutory law is particularly striking, which is the exact cause of the problem with criminal law regarding the crime of illicit computer system access [5].

First and foremost, incomprehensiveness is an unavoidable defect of criminal legislation. Since the enactment of the Chinese Criminal Law in 1997, despite the amendments it has undergone to make it relatively complete, it has still not been capable of circumventing the feature of incomprehensiveness of the statutory law, which is precisely the major reason why hierarchical protection mechanisms for computer information systems are lacking. As previously mentioned, the legislator attempted to create a hierarchical protection system for computer information systems through the crimes of illegal intrusion into computer information systems in the first clause and illegal acquisition of computer information system data and illegal control of computer information systems in the second clause of Article 285 of the Criminal Law. The earlier offense restricts the target to computer information systems used in government, building national defense systems, and cutting-edge science and technology, and its establishment merely requires the commission of illegal intrusion. On the contrary, the latter crime stipulates that for computer systems in ordinary fields other than those mentioned above, It is essential to avoid illegally accessing computer systems, taking control of them, or obtaining data from them, thereby constituting a crime. From these, it is apparent that the original intention of the legislator was to implement focused protect computer information systems in critical areas while implementing general protect computer information systems in ordinary areas. Nevertheless, given the complexity of the objective situation, the system of crimes meticulously constructed by the legislator tends to be ill-conceived, thereby frequently failing to achieve the desired legal effect. On the one hand, other priority areas, such as

DOI: 10.54254/2753-7048/17/20231216

economic construction and social security, as important as the three computer information systems mentioned above, whereas the enumerated legislative approach adopted in the first clause of Article 285 of the Criminal Law fails to encompass these areas, which means that these critical areas cannot be prioritized for protection. On the other hand, in objective reality, the wrongdoer may not only illegally intrude into the computer system in the critical area, but also may further illegally obtain the data in the system or illegally control the system, while these two situations are precisely neglected by the legislators. The result of this lies in the emergence of the above-mentioned poor legislative logic described by the author. As a result of the exclusion of the three major computer information systems from the additional clauses 2 and 3 of Article 285 of the Criminal Law, the criminalization of intrusion into computers of national important level remains at the level of intrusion, which appears to manifest the seriousness of the crime by the standard of conduct offense. It has failed to provide more perfect legal protection to the three major important computer information systems as it should have been. Such a legal effect is exactly opposite to the original intention of the legislators. In this way, it can be noted that criminal legislation does not always express or exclusively express the subjective meaning of the legislators, while the incomprehensiveness of Article 285 of the Criminal Law has led to the fact that the hierarchical protection system of computer systems has not been and cannot be thoroughly implemented.

4. The Solution to the Issue of Judicial Application and Suggestions for Improving Legislation

4.1. Accurately Identify the Scope of the Crime Object and Expand the Judicial Interpretation of “State Affairs”

The author believes that a judicial interpretation can be issued to include “computer information systems of state organs or public services in the fields of finance, telecommunications, transportation, education, medical care, energy, and other fields” into the computer information systems of “state affairs” based on the aforementioned judicial practice and legislative analysis, to encompass the computer information systems of the vital economic construction and social security fields in China.

The scope refers to Article 4 of the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Endangering Computer Information System Security promulgated by the Supreme People’s Court of the People’s Republic of China and the Supreme People’s Procuratorate, which has come into effect since 1 September 2011, defining “destroying the operations, information, or software of government agencies or computer information systems that deliver public services in the sectors of finance, telecommunications, transportation, education, health care, energy, etc., and having a significant adverse effect on human life and/or production.as being the circumstance of “particularly serious consequences” of harming computer information systems. From the legislation of various countries, the most common situation in which criminal law establishes aggravating provisions is when computers critical to the operation of infrastructure such as banks, communications, health services, public services, or government agencies are illegally hacked, especially when it involves computers managed by the state or related to the operation of critical infrastructure [6]. In comparison to the cybercrime legislation in the United States, the criminal object of the crime of illegal intrusion into the computer information system in China is determined to reflect a number of shortcomings: Article 1030 of the United States Code (Fraud and Related Activity in Connection with Computers), in which clause (a) stipulates four kinds of crimes of illegal intrusion into computer information systems, which are (1) intrusion into a computer information system to obtain information, (2) intrusion into a computer information system to obtain a benefit to obtain property by fraud, (3) illegal intrusion into a national computer

DOI: 10.54254/2753-7048/17/20231216

information system, and (4) illegal intrusion into a computer system to obtain confidential state information and disseminate or withhold it [7]. In contrast to the legislation in China, there is also no restriction on the computer information systems protected by the aforementioned Article 1030(a)(2) of the United States. As long as the data being accessed belongs to a US government department or agency, is stored on a secure computer, or is financial data from a bank or consumer reporting agency, including the computer information systems of various Internet companies or individuals that provide general or special network services to U.S. government and related agencies, all of which can become the subject of protection under this crime. In comparison, the aforementioned criminal legislation of the United States regulates a broader crime object, and extends to the subsequent further infringement of computer information system data, with heavier penalties. From the perspective of the legislative effect, the aforementioned crime legislation in the United States provides more specific and detailed provisions, which can not only achieve a high degree of protection of critical areas of computer information systems but also be capable of severely cracking down on intrusive behavior for the sake of implementing illegal activities, which has preferably avoided the overly broad crackdown on communication-related crimes that impede the normal development of the information society [8]. In contrast, the identification scope of "state affairs" computer information systems in China has been excessively narrow, which is not only incompatible with the speedy development and wide application of computers and networks but also fails to play an adequate legal protection role in the information systems related to national economic construction and social life, such as finance, electric power, communication, transportation, medical care, etc.

4.2. Add Data Protection Provisions for Significant Computer Information Systems, Establish the Independent Status of Data Crime

The author contends that adding an impartial data crime perspective can effectively address the problems with China's criminal law legislation on computer information system crimes. For the sake of reinforcing the independent protection of critical data security, a more stringent and meticulous system of crimes that further endanger data security acts in the field of three major computer information systems should be set up. In case of serious consequences for the deletion, addition, and modification of network data in violation of national regulations, the establishment of the crime of damaging data of three major computer information systems should be probed for special regulation, to bridge the loopholes in the regulation of data crimes in criminal law, and dissolving the dilemma of judicial practice in cracking down on such data crimes. The legal interests protected by the crime of illegal intrusion into computer information systems in the Criminal Law of China cover merely the establishment of integrity and security of computer information systems, which is specifically intended to sanction crimes that cause intrusion into the three major computer information systems, while excluding the protection of data security therein [9]. It has been challenging to achieve the prevention, deterrence, and punishment of criminal acts of illegal intrusion into significant computer information systems because, in the case of the crime of further interference with data after unauthorized access, there has been no additional effective penal code for such behavior with serious social harm. The computer system and its stored information itself are merely a massive collection of data [10]. By the principle of compatibility between crime, responsibility, and punishment, the author believes that China can establish a separate crime in the future amendments to the criminal law for intrusion into the three major computer information systems, and further interfere with data security, with details that can refer to the foreign criminal law system for cybercrime. For instance, the German "data-centered" cybercrime criminal system can be referred to. The German Criminal Code criminalizes cybercrime, including the following six crimes: the crime of snooping on data, the crime of intercepting data, the

DOI: 10.54254/2753-7048/17/20231216

crime of preparing to snoop and intercept data, the crime of harboring data, the crime of altering data, and the crime of damaging computers [11]. Its scope of data security protection is comparatively comprehensive, with clear descriptions of the criminal provisions and accurate definitions of terms, whose legislation and its successful experience in judicial practice are of value to China. Even though computer information systems and data security are both new legal interests that require protection in the context of the progress of the times, the confidentiality of data should remain the key legal interest to be protected. The reasonable use of the normative interpretation function of the legal interest of "confidentiality and usefulness of data content" can enable partial controversial data crime cases to be processed appropriately to the greatest extent. In addition, it is imperative to further improve the criminal legislation on cybercrime in China, to attach importance to the safe operation of computer systems, while taking into account the criminal legislation on data security of the three major computer information systems, thereby underlining the protection of data security and more effectively satisfying the need to curb the current trend of the spread of cybercrime.

4.3. Increase the Range of Statutory Sentence

At present, the crime of illegal intrusion into the computer information system involves a single type of penalty and a relatively lenient sentencing range. It is only by appropriate increase in the statutory sentence range for this crime that the principle of proportionality between crime, responsibility, and punishment in criminal law can be better implemented. Given the degree of privacy and usefulness of the data included inside the three main computer information systems, the legal interests violated by the crime of unauthorised access to computer information systems are significant. Moreover, the basic strategy of preventing cybercrime should be "hit early and hit small", as well as the comprehensive consideration of criminal jurisdiction, the legislation of the United States in this regard can be referred to. The crime of illegal intrusion into the national computer information system is defined in Article 1030(a)(3) of the United States Code, which refers to the intentionally unauthorized intrusion into the non-public computer information system of a state department or agency of the United States, which is used exclusively by the United States government, or where there is non-exclusive use, is in use by or for the United States government, while such intrusion affects the above use or service [12]. The difference that can be drawn from for reference is that this clause of the crime provides for a felony type to punish attempted offenders [7]. In addition, the additional property penalty for the perpetrators of crimes that cause serious economic losses is commensurate with their illegal proceeds to improve the effectiveness of the penalty. Cybercrime is mostly motivated by profit, while only the configuration of property penalty can improve the cost of crime and effectively curb the criminal impulse.

5. Conclusion

The crime of unauthorized infiltration into computer information systems is anticipated to constitute a serious threat to societal well-being, economic growth, and national security as a new sort of crime. In this regard, it is imperative to develop a new interpretation of this crime, to appropriately expand the scope of the crime object, to moderately increase the range of statutory sentences, and to timely introduce relevant judicial interpretations to prevent and punish this crime effectively, consequently ensuring the safety of China's computer network and information system. On the basis of drawing on previous views on the judicial determination of the "three major computer information systems", The author highlights the shortcomings in China's criminal legislation regarding unauthorized access to computer information systems. On the issue of cross-regulation of the first and second paragraphs of Article 285 of the Criminal Law, and the weak application of the

DOI: 10.54254/2753-7048/17/20231216

first paragraph in judicial practice due to the unclear extension of "state affairs", the author proposes an explicit definition of the judicial interpretation of "state affairs", which will make it easier to apply legal doctrine and academic research, as well as meet the need to develop criminal law in the context of the current cybercrime situation.

References

[1] *Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.*

[2] *McQuade, S. C. (2006). Understanding and managing cybercrime. Boston: Pearson/Allyn and Bacon.*

[3] *Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2, 13-20.*

[4] *Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses.*

[5] *Broadhurst, R., & Chang, L. Y. (2012). Cybercrime in Asia: trends and challenges. Handbook of Asian criminology, 49-63.*

[6] *Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Vol. 4). Polity.*

[7] *Okutan, A. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287-294.*

[8] *Bossard, A., & Office international de justice criminelle. (1990). Transnational crime and criminal law. Office of International Criminal Justice, University of Illinois at Chicago.*

[9] *Libo, Z. (2021) On the Criminal Law Protection of Network Security.East China University of Political Science and Law, DOI: 10.27150/d.cnki.ghdzc. 2021.000030.*

[10] *Li, D. (2022) A Comparative Study of the Criminal Law Regime of Pure Cybercrime. Beijing Foreign Studies University, DOI: 10.26962/d.cnki.gbjwu. 2022.000009.*

[11] *Wenyuan, Q. (2022) The Application and Reflection of the Criminal Policy of Hitting Early and Hitting Small in the Context of "Less Arrest and Careful Prosecution and Detention" --Taking Cybercrime Governance as a Perspective. Tribune of Political Science and Law, 40(02): 62-73.*