Study on the Legal Status of Computer Network Crime and Its Legal Prevention

Shuangxi Zhong[1, a], Min Zhang[2, b]

[1,2] Jiangxi University of Traditional Chinese Medicine, Nanchang, JiangXi, 330004

[a] email:zshuangxi@126.com,

[b] Corresponding author,email:zhangminrd@126.com

Keywords: Computer Network Crime, Legal Status, Legal Protection

Abstract. In the 21st century, the rapid development of the computer, and the development of computer largely changed people's daily life, work and learning. For computer network, its security is often affected. For example: computer network crime, it makes the computer's security by a large degree of influence. Based on the analysis of computer network crime laws targeting on further exploration for computer network crime law protection policy, in order to provide some valuable recommendations for computer network security can be improved.

Introduction

Development of the Internet to people's daily life, study and work to bring the convenience, but there are some security risks, especially under the influence of network viruses and hackers, making the network more and more frequent criminal acts. Obviously, due to the presence of computer network crime, making the security of the computer network saturation test [1]. Strengthening the security of computer networks, computer networks to promote the sound development point of view, the paper "Computer Cybercrime Law and Legal Measures Against Positioning" research is significant.

The Legal Status of Computer Network Crime

For computer network crime, it is a new phenomenon of crime in the context of development of the Internet generated. From the early academic concepts, the show cybercrime as visible criminology, rather than the scope of the criminal law. But in 1997 China's Criminal Law clearly stipulates pawn: the crime of illegal intrusion into computer information systems and information systems undermine the crime, in most cases, cybercrime. Therefore, from the point of view of criminal law, cybercrime mentioned, essentially refers to two charges, including criminal behavior [2]. In the 21st century, the rapid development of the network in the background, to the general criminal network based on the development of China's criminal law has to a certain extent. From many angles, the computer network crimes attributed to the criminal law areas. And the need to be clear that computer crime and cyber crime are two concepts can not be confused.

From the characteristics of computer network crime point of view, the presence of intelligence, obvious behavioral characteristics, criminal means diversity and extensiveness transmission range. And, as long as the computer network have a certain understanding, it is not difficult to understand its characteristics. In intelligence, for example, refers to a computer network offenders usually have strong logical ability, and rich in the field of computer expertise. In addition, for the computer network crime, its forms of crime three major categories: one is the spread of network viruses; the other for phishing; thirdly to online pornography. First, network viruses, it belongs to a class of traditional forms of cybercrime, there is great harm. Such as the early "Panda" virus, that is, through multiple variants, and with the complexity of the virus, these viruses spread fast, it will cause great economic losses. Secondly, phishing, means that by a similar design of the site, users will be attracted, then the user's privacy is acquired, further steal a user's credit card, bank account and phone number, and then carry out criminal activities [3]. In addition, Internet pornography, the

spread of pornography through the website pictures, video and other health effects, major Internet pornography on young people, causing a problem for the young people living and learning. All in all, in order to ensure the security of computer networks, it is necessary in the case of a clear understanding of its definition of the crime, the characteristics and methods, to take effective preventive strategies.

Legal Protection Policy for Computer Networks Crimes Inquiry

In the above analysis, the computer recognized the related cybercrime legal positioning. In order to make the security of computer networks can be improved effectively, it is necessary to have specific laws for computer network defense strategy crimes, specific strategies are as follows:

For computer information systems, early in 1994 our country will be promulgated the "People's Republic of China Information System Security Protection Ordinance." Under the law and gradually improve the situation, further promulgated the "Internet electronic bulletin service management requirements," [3]. Although China promulgated a computer network for the corresponding legal provisions, but the pace of development of the Internet very quickly, often face legal provisions difficult to adapt to the situation of development of the Internet, in the absence of immediate, targeted legal provisions as the case of security, would potentially kinds of security risks. Therefore, there will be necessary to build a comprehensive network security legislation system. For legislative bodies, the need to pay attention to the key elements of legislation, combined with valuable experience of western countries in terms of Internet legislation to make the Internet more legislative norms, standards. On the one hand, it is necessary to meet the basic legal development of the Internet to build, enrich the content of the law. On the other hand, for Internet safety legislation constructed, to be able to play a role in the fight against cybercrime, and to a certain extent be constraints on cybercrime. In addition, there is a need to strengthen cybersecurity legislation to strengthen exchanges with foreign countries, further improve our network security legislation effectively promoted.

For computer network crime, from China's "Criminal Law" point of view, in Article 285, in two hundred eighty-six and two hundred eighty-seven clearly defined [4]. However, in the continuous development of the Internet and computer networks more types of crime continues, the conventional laws can not begin to fully adapt to the constraints of cybercrime and bundles. Therefore, it is necessary to perfect the criminal legislation, on the one hand the need for the name of a unified computer network crime. From the domestic point of view the current laws and regulations, adopted a "computer information system" and replace the basic concepts from the current "computer information network" and "Internet information technology". To make the computer information network specific content even more clearly, we need to clear the domestic Internet, but also need to clear the Internet, under the name of the unified specification conditions, and thus the extent of regulation before we can make laws and regulations be effectively improved. On the other hand, we need to be clear on the unit crime. From the current situation, whether in personal funds or are technically limited, while the unit is a computer crime cybercrime more general way, it is necessary for the relevant criminal law crime unit be set up, the unit will be included in corporate computer among the main crime, the legal code of conduct unit, the control unit occurs in the form of computer network crime events. In addition, there is need to implement qualifications, namely computer network crime against people, according to the seriousness of the offense, it may be right to give the deprivation of network services, so that people can not participate in the crime network activity, then control cybercrime Happen again. And may also take criminal property strategy to financial penalties as a foundation for the computer network to reduce the offender's economic capacity, and learned to play the role of economic punishment, and thus make the recurrence of cyber crime has been effectively controlled.

"Preventive measures" ideological emphasis on prevention and control of adverse events. For computer network crime, the possible control of its occurrence is critical. Therefore, it is necessary to strengthen the enforcement of the law enforcement agencies. On the one hand, strengthening of law enforcement, namely a strong professional organization of police network [5]. For computer

network crime, the obvious characteristics, diversified manner, thus building a network police force process, the need to strengthen the squad members training in knowledge and technology, so that each member of a professional police force capable of fully qualified for the job. On the other hand, the need to increase funding for law enforcement agencies to promote the strengthening of law enforcement, Internet police do need to be aware of the importance of law enforcement network, and clarify its role in the actual work process, focus on their own resourcefulness and the ability to solve the case improved. All in all, the need to promote the strengthening of law enforcement agencies, law enforcement, police do a good job from the network, I believe on the basis of a computer network to maximize the prevention of crime incidents, the security of the computer network will be able to be effectively improved, and thus for the user's information security and property to provide effective protection.

Conclusion

By exploring this article, the computer recognizes the dangers of cyber crime, computer network in order to control the occurrence of crime, thereby improving the security of computer networks, it is necessary to build a comprehensive network security legislation system, and to improve criminal legislation to further promote law enforcement strengthening of law enforcement agencies. I believe the above aspects to be improved, the occurrence of criminal computer networks will be able to obtain a large degree of control, thereby enabling the security of the computer network has been effectively protected.

References

[1] Chen Yongsheng. Computer Network Crime and Criminal Procedure Challenge and response system [J]. Science of Law (Journal of Northwest University of Politics), 2014, 03: 140-153.

[2] Huang Ziqi. Cybercrime Analysis and Prevention Strategies [J]. System and Society, 2012, 23: 234-235.

[3] Pi Yong. Cyber-Terrorism Crime and the overall legal countermeasures [J]. Global Law Review, 2013, 01: 6-20.

[4] Xu Hanming. ZhangLe era of big data and Punishment Thoughts financial crime prevention network [J]. Economic and Social Systems, 2015, 03: 11-19.

[5] Yu Zhigang. Participate in the conclusion of the International criminal networks China stance [J]. Tribune, 2015, 05: 91-108.