Research of Computer Network Crimes Investigation and Legal Supervision Measures

Shijie Zhu[1, a]

[1] East China University of Political Science and Law, Shanghai, 201620

[a] email

Keywords: Computer Network; Criminal Investigation; Preventive Measures

Abstract. In recent years, the rapid development of computer networks has become an indispensable part of human life, and now, more and more people use mobile phones, computers and other electronic devices online, and mobile phones and other electronic mobile devices are constantly updated and developed in. The extensive use of the Internet not only facilitates people's study, life and work, but also inevitably there are some security issues, some criminals have begun to use computer networks to carry out network scams to commit crimes, the convenience and spread of the Internet as their perpetrators Tools, to social order and social moral civilization caused a certain degree of threat. Based on the analysis of the level and characteristics of computer network crime, this paper puts forward countermeasures and preventive measures for the computer network crime investigation.

Introduction

With the continuous development of science and technology, the development of computer network is more and more rapid, in a number of areas to promote social development and progress [1]. However, at the same time, network technology is also a double-edged sword, the advantages and disadvantages coexist, criminals through the development of network technology to carry out illegal and criminal acts of law and order and social development have a negative impact. Therefore, to deal with such illegal acts, we must first correctly understand the illegal behavior and identify the crime, its effective investigation, to take positive and preventive measures to suppress the behavior and to stop, to take all possible means to maintain social stability, to ensure the stable development of society. It is also important to strengthen international cooperation, promote the peace and stability among countries, promote the globalization of economy and science and technology, and have certain legal effect on the investigation of computer network crime [2].

What is Cybercrime

Cybercrime, as the name suggests, is the use of today's high-tech means to computer as a medium, with the spread of network technology and convenience on the network for fraud, attack, destruction and other means of illegal acts. Cybercrime includes not only man-made computer network module programming, man-made password operation, not in accordance with the legal procedures to crack passwords and other acts, but also criminals use network vulnerabilities network intrusion behavior. Therefore, only by correctly understanding and identifying the network illegal procedures, directives, websites and other means, and promptly carry out legal sanctions against them, so that the network can not be found, the network technology is very difficult to be found, the network technology is highly disseminated, spread fast and destructive, To a certain extent, to prevent it. Therefore, to strengthen the computer network to solve the problem of criminal investigation and take effective legal supervision measures are urgently to be solved and implemented [3].

The Characteristics of Cybercrime

The network crime means is diverse, is not easy to discover, has the very big difficulty in the

investigation aspect, needs to involve the massive each area personnel to cooperate, but achieves the effect not to be satisfactory, therefore, the related personnel must aim at the network crime behavior characteristic, The following are some of the characteristics of computer network crime. Only the correct understanding of the characteristics of cybercrime, it can be in technology and methods to update and reform.

Diversity of criminal methods. With the development of network technology, network hacker personnel technology is also advancing with the times, and advanced crime, they usually use the most advanced technological means of the community to carry out crimes. Behavior, they can make the site through the temptation to point to the community for fraud, but also by way of advertising to join the site window.

Concealment of criminal acts. Cybercrime is usually carried out through the spread of the network, the process of cybercrime can be completed in a short time activity, in a few minutes or even seconds to be completed, it is difficult to be aware of human beings, with a strong covert, Difficult to be found. Criminals commit crimes, only through the keyboard to the computer to enter the appropriate instructions or procedures, you can conduct acts such as criminal fraud, a short time horizon, the computer network system hardware and software will not cause damage, it is not easy to be Find. In addition, the criminals are not restricted places of crime, can be remote control, so in the country or cross-border networking, criminals can at any time and any place to commit crimes.

At present, most of the computer network crime is the use of high-tech technology, and through careful design, even if found to have signs of criminal behavior, can not be found in time and the implementation of legal means to impose sanctions.

Network investigation and evidence collection is difficult. Most of the crimes in the computer network communicate with each other through Internet or wireless. The current network technology is developed. Although the current detection technology can track and record these behaviors online, it can effectively diagnose cybercriminals by using the current electronic camera. . However, due to the large number of proxy servers and the complicated data on the network, the crime information can not be effectively identified. Most cybercrime acts are carried out by modifying the intangible information such as procedures and changing data.

Transnationality of cybercrime. With the development of the globalization of the world economy, the cybercrime has become more and more rampant, the network around the world, criminals to criminal means to facilitate, so there is no border control of criminal control, so that even if the confirmation of criminal acts As well as the modus operandi, can not be the first time to stop their criminal acts. Irrational criminal acts involve many countries, and the relationship between the international community can cause a certain degree of damage. National leaders should pay attention to strengthening the use of the mass media functions, the absconded domestic computer network of criminals worldwide notice, widely spread the world of Chinese, determined not to miss any one criminal.

Network Crime Investigation Program

Cybercrime acts in a variety of ways, the means of detection to catch up with the speed of criminal acts can change the speed of criminal behavior to combat containment [4]. The following is a number of detection methods for cybercrime, the actual application of the detection program has yet to be further updated and developed.

Reproduce the crime scene, the use of detection strategies. Computer network crime cases, the most important way to solve a crime is to simulate the scene, the relevant staff to use their experience to detect them. Among them, the simulation of the crime scene must be completely consistent with the criminals invasion of the scene, the relevant network of criminal investigators to detect trap design, and to make it the normal work cycle, with the timely detection of unsafe sites, advertising, Information and other functions, of course, in the process of setting the trap investigation, the computer system can not have the original system damage factors, and can protect the computer hardware and software information. In the simulated crime scene to find the corresponding solution to the problem of cybercrime and can be applied to the actual detection.

Make full use of electronic means of evidence. Electronic forensics plays an indispensable role in the investigation of criminal behavior, electronic evidence has many characteristics, electronic evidence with concealment and retention, can be a long time to save the information. Although the means of electronic forensics in China is still in the stage of development, but in the field of application has been very extensive, and China should strengthen the electronic forensics research and development in the field of computer network crime detection more widely. Computer network crime as long as the storage through the computer and the direct use of computer crime, therefore, the relevant law enforcement officers from these two aspects of crime for the detection of the start, by strengthening the computer storage devices to improve, strengthen the computer The use of the control. For example, to strengthen the management of identity information, each computer network users to use the computer before the registration of their identity information, waiting for approval before they can effectively enter the computer network platform.

Electronic evidence means not only to the required electronic information to investigate, save, send, copy, etc., but also a clear and reasonable reflection of the scene, the detection of law enforcement officers play a crucial role. The only requirement for electronic forensics is the quality to be the appropriate protection, integrity and authenticity is an important guarantee for electronic evidence, to get the relevant judiciary identification can be put into use, and thus indirectly promote the electronic forensics technology And development.

Strengthen the Management of Computer Networks

Strengthening the computer network management is an important means to prevent computer network crime, many computer viruses are due to the lack of the corresponding management system, do not do the first line of defense computer, so that the relevant computer viruses can easily and easily invade Related computer, to achieve the purpose of theft and intrusion.

Strengthening the capacity of investigators. With the development of network technology, human intelligence is developing with the development of the times. Therefore, more and more professional knowledge and social skills can be applied to the computer network crime detection strategy to solve the criminal events more effectively. Relevant law enforcement units should regularly on the unit staff within the legal and moral knowledge transfer, and should pay attention to with a large number of legal professionals. The relevant law enforcement officers can not only know the law, abide by the law, understand the law, but also familiar with the mastery and operation of various computer field operations, such as encryption, decryption, editing programs and other knowledge and skills. In addition, it is necessary to strengthen the law enforcement officers of the equipment and detection technology [5].

Strengthen the legislative rules and systems. The current computer network crime is mainly through the computer field of the extensive and popular information stealing, invasion, copying and other means of crime. Cyber crime is convenient, does not require a lot of manpower and resources, but the need for advanced technical means, the need for professional and technical personnel, crime locations with great uncertainty, therefore, the relevant law enforcement officers can not be personal arrest, the relevant state leaders To this kind of phenomenon for the development of laws, the development of specialized computer laws and regulations, the network of criminals to justice.

Actively strengthen international cooperation. Criminal acts are not national boundaries, some criminals in foreign countries can have complete control of a series of domestic criminal acts, which makes the crime even more rampant, want to solve such problems, our country should actively participate in international cooperation, The establishment of China and other countries between the laws and regulations, so that criminals in any country can not survive, we must always accept the legal sanctions to safeguard the stability of the country. Countries should be closely linked, the unity and cooperation between countries, cooperate with each other to combat international criminal forces, for the suspects collected evidence, to immediately detain or extract the relevant evidence of physical evidence.

Conclusion

With the development of science and technology and the rapid progress of globalization of network and economy, more and more cybercriminals are threatening the social harmony and stability. Therefore, only when relevant policies and laws and regulations are imposed can these sanctions be imposed, In addition, the relevant law enforcement officers in conjunction with relevant national technical means to stop the behavior of cyber criminals and hackers, set up in the network security access security settings, so that hackers can not normally invade the regular site. Combating cybercrime technology can only stop hackers by keeping up with the times. In addition, the network detection tools to be updated, forensic staff should also pay attention to strengthen the training of their own investigation ability and judgment. In order to solve these problems, we should strengthen the automation performance of computer network crime investigation to solve the defects of human judgment. International cooperation should be strengthened between the degree of common to maintain social and international stability.

References

[1] Chen Yongsheng. Computer cybercrime's challenge to criminal procedure and system response [J]. Journal of Northwest University of Political Science and Law, 2014, 32 (3): 140-153.

[2] Gu Yanlin. Application of computer forensics technology [J]. China Management Informationization, 2012, 15 (4): 65-67.

[3] Wu Mingsheng, Li Huanhuan. Electronic evidence in criminal proceedings in the authenticity of the judge and its effectiveness [J]. Journal of Railway Police College, 2013, 23 (5): 86-88.

[4] Cai Xiaolian. Data backup and recovery in the computer network of criminal investigation [J]. Information Security and Technology, 2014, (8): 79-82.

[5] Wang Gang, Bai Wei. The public security organs for network gambling case investigation and evidence collection [J]. Law and Society, 2012, (30): 77-78.