Journal of Global Information Management
Volume 30 • Issue 7

Big Data Security Management Countermeasures in the Prevention and Control of Computer Network Crime

Hongning Wang, Jilin University, China*

ABSTRACT

This paper aims to study the countermeasures of big data security management in the prevention and control of computer network crime in the absence of relevant legislation and judicial practice. Starting from the concepts and definitions of computer crime and network crime, this paper puts forward the comparison matrix, investigation and statistics method, and characteristic measure of computer crime. Through the methods of crime scene investigation, network investigation, and network tracking, this paper studies big data security management countermeasures in the prevention and control of computer network crime from the perspective of criminology. The experimental results show that the phenomenon of low age is serious, and the number of teenagers participating in network crime is on the rise. In all kinds of cases, criminals under the age of 35 account for more than 50%.

KEYWORDS

Big Data Security Management, Computer Network Crime, Countermeasure Research, Crime Prevention

1. INTRODUCTION

With the development and popularization of network and information processing technology, the subjects involved in computer network crimes have become increasingly non-professional, younger, and the types of crimes are becoming more complex and diversified. Judging from the analysis of research papers on the Criminal Procedure Law in recent years, the current research on computer crimes and cybercrimes is in an ascendant stage, but judicial practice lacks the support of corresponding legislation and theoretical research. Relevant research mostly starts from a certain aspect of network security and criminal law, such as network protection, criminal types of criminal law and related criminal law provisions or from a purely technical perspective such as the construction of a certain network technology to prevent intrusion. However, there are not many materials to study computer crime and cybercrime from the perspective of criminology. Most research materials often divide computer crime and cybercrime into two different concepts to study. This is bound to give people an illusion that computer crime and cybercrime. Cybercrime is two different crimes, and their scope and conviction and punishment are naturally different. But I believe that if there is no network, there will be no computer crime. Because of the lack of network interconnectivity, a single computer is at best a data processor, word processing tool, or a large-capacity storage device for storing information (Namasudra, 2018). From this perspective, the research on this type of computer-related crimes can also

DOI: 10.4018/JGIM.295450 *Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

be attributed to traditional crimes. Infringement of computer ownership, computer theft, criminal use that violates the personal rights of citizens, crimes of infringing privacy through computer networks, etc., or crimes of infringing on commercial secrets and important information.

On the other hand, if there were only networks and no computers, the so-called cybercrimes or computer crimes would never happen today. The existence of the network did not follow the birth of the computer. The birth of the network was earlier than that of the computer. Today, computers and networks have merged into an indivisible whole, an organic part of cyberspace. In this organic whole, in addition to computers and network hardware equipment, there are also system platforms, software that support the operation of computer network systems, information processing, and various information sources that exist on the Internet and are exchanged and transmitted (Parada, 2018). These are indispensable of the components. It is precisely because of the diversification and complexity of these factors that computer network crimes are almost all-encompassing.

In view of the far-reaching impact of computers on social life and the seriousness of computer-supported crimes infringing on legal interests, the existing fruitful research results on computer crimes are still difficult to meet the requirements of regulating computer crimes, and more people should come to study them. Computer crime, with the continuous development of computer technology, the influence of computers on society continues to increase, and more and more traditional crime fields also involve computer operations. There are currently several cases of theft through illegal modification of computer system data, and similar situations abound. Therefore, it is reasonable to say that computer crimes or computer-related crimes should become one of the core issues of criminal law research. Caring about computer crimes is caring about the future of our society.

In order to define the object of legal protection of cybercrime, Lux L M critically reviewed the hypothesis that cybercrime protects specific computer-related interests in the article (Lux, 2017; Gao, 2017). On this basis, it is pointed out that if these crimes involve the use of computer networks in addition to affecting computer software, then it is reasonable to recognize the benefits of these characteristics. The study reflects that computer systems are the free development of individuals and institutions in the democratic rule of law. The function performed. However, this work did not rigorously examine the argument that computer crimes protect specific legal assets that are properly computerized. Rashkovski D introduced, discussed and analyzed Macedonian legislation on cybercrime on specific cases commonly encountered in practice and international standards related to cybercrime. Focus on the introduction and analysis of the Internet Crime Complaint Center and the Macedonian Ministry of Internal Affairs on Macedonian cybercrime complaints and reports on victims. In addition, it also highlights several recent cyber crime cases reported by Macedonia (Rashkovski, 2016). However, this situation can be improved by including the Macedonian authorities more actively in the global response to cybercrime, and by implementing more robust cybercrime prevention measures and strategies. Lee L has conducted research on various forms of cybercrime, and observed that the original static webpage network has become an evolving information ecosystem (Lee, 2019). And put forward that in ensuring the development of corporate cyber security strategy, there are five key elements: collaboration, evaluation, development, application and apprenticeship. However, huge changes have brought huge opportunities-malicious hackers have not been slowly exploited.

The innovations of this article are: (1) Computer network crime prevention is based on the clarification of the concept of cybercrime, by investigating and analyzing the form and characteristics of cybercrime, analyzing the causes of cybercrime and summarizing the previous theoretical results and practice based on experience, and submit governance opinions and suggestions. (2) Through the analysis of several typical computer network crimes, we propose to observe the problems of computer network crimes from the perspective of criminology.

2. METHOD OF OBSERVING THE MAIN FORMS OF COMPUTER NETWORK CRIME FROM THE PERSPECTIVE OF CRIMINOLOGY

2.1 Concepts Related to Computer Cybercrime

(1) The concept of computer cybercrime

Computer cybercrime is the use of computer technology to attack systems and information, destroy the network or implement other network-assisted crimes (Aaron, 2018; Eboibi, 2017). From the perspective of specific criminal methods, computer network crimes include criminal acts in which criminals use technologies or tools on the Internet to program, encrypt, and decrypt (Parah, 2017). It also includes crimes committed by criminals using software instructions, network systems and product encryption, as well as other technical and legal loophole crimes inside and outside the network. It also includes criminals using network service providers (such as ISPs, ISPs, etc.) on network systems. Network providers and ICP network information providers) commit crimes or other specific circumstances (Xie, 2020; Orji, 2019).

Computer network crimes can basically be divided into two categories (Boddy, 2018). One is the crime of disrupting the network and information security, and the other is the use of the network to commit other crimes. In other words, the first type of crime is a crime that uses a computer network as a criminal target, and the second type of crime is a crime that uses a computer network as a means of crime.

(2) The difference between computer network crime and computer crime

Some scholars believe that computer-related crimes are all computer crimes. According to the definition of computer crimes, it can be seen that some computer network crimes conform to the characteristics of computer crimes and are all computer-related crimes. However, computer network crimes infringe object is network information and information security, while the object of computer crime is computer system and computer information (Richardson, 2020; Stearns, 2018). From this point, it can be seen that there are essential differences between computer network crime and computer crime, and the connotation and extension of the infringement object are different.

(3) The difference between computer cybercrime and cybercrime

Computer cybercrime emphasizes crimes committed with computers as criminal tools, and the tools used in crimes must be computers, while cybercrime does not emphasize the tools used in crime (Maher, 2017). This means that computers do not have to be used as criminal tools for crimes in cyberspace, but other tools can be used to commit crimes. For example, mobile phone cybercrime and other electronic products that can be used as criminal tools to commit crimes on the Internet.

(4) The characteristics of computer network crime

1) High intelligence of the criminal subject. Cybercriminals have high professional knowledge, can master computer technology, can easily bypass security surveillance, and can well hide criminal activities (Hinchliffe, 2017).
2) The concealment of criminal acts. Due to the characteristics of computer networks, such as transparency, uncertainty, etc., computer network crimes are much concealed (Hert, 2018).

3) Cross-regional crime. Computer cybercrime is not restricted by traditional crimes and other geographical restrictions, and has shown a trend of internationalization (Lloyd, 2020; Rock, 2017). The Internet is characterized by "compression of time and space". When various information is transmitted through the network, the border and geographic distance disappear, and the possibility of cybercrime is created between the region and the border. As long as their computers are connected to the Internet, criminals can carry out criminal activities anywhere on the network, and such crimes are not restricted by geographical areas. Therefore, the concealment is strong, the detection difficulty is quite large, and the harm is also very great.
4) Rejuvenation of criminal subjects. Cybercrime is dominated by young people under the age of 35. People in this age group have just left their families and parents and have a lot of free time at their disposal. They are curious about new things, hackers, viruses, etc. New things are full of yearning, coupled with a weak sense of law; it is convenient to use their computer knowledge to embark on the road of crime (Li, 2017). Juvenile delinquency has always been a social problem. Because computer networks are filled with a lot of pornographic and violent information, many young people with poor self-control ability are easily affected by it and eventually go to the road of crime.
5) Serious social harm. The social harm of cybercrime is easily overlooked by people. Nowadays, more and more online financial theft, online fraud, and the dissemination of pornographic information on the Internet make people gradually realize the harm that computer network brings to personal life (Poltavtseva 2019). However, the social harm caused by some cybercrimes is actually difficult for everyone to see, and even criminals are hard to predict. The harmfulness of computer network crime is no less than that of ordinary criminal behavior, and even more harmful to society than ordinary criminal behavior.

2.2 Computer Crime Comparison Matrix

This matrix can be divided into three types of computer crimes from the analysis of criminal subjects: intruders, thieves and saboteurs (Riek, 2016; Kouttis, 2016). The computer crime comparison matrix was originally designed by the Federal Bureau of Investigation (FBI) (Laviero, 2016). Out of the need to construct a model, it also provides four aspects of organizational characteristics, operational characteristics, behavioral characteristics, and resource characteristics for each criminal subject. Make a characteristic description. It should be noted that this crime comparison matrix is mainly to enable us to grasp the method, not to provide conclusions. For example, in this matrix, in terms of behavior characteristics, a very useful column is listed: Potential Weakness Column (Mazurczyk, 2016). It believes that the potential weaknesses of the three different criminal subjects are different. For example, the biggest weakness of group intruders is that there are many people and it is difficult to keep secrets; while individual intruders have a strong desire for performance. Self-reliance is high and strong, bragging.

2.3 Feature Metrics

(1) Cluster coefficient

The cluster coefficient is called the clustering coefficient. It is usually a measure of the degree of network grouping, and it is also an extremely critical parameter (Singh, 2020; Hardik, 2018). In terms of social networks, the form of grouping is a very important feature of the cluster coefficient, and grouping is also called the phenomenon of clustering. The cluster factor C_i of node i represent the connection relationship between nodes directly connected to this node in the network. Therefore, the

clustering factor C_i of node i also refers to the ratio of the number of edges that can exist between the node and its neighbors to the maximum number of edges that can exist, and the expression of C_i is:

$$C_i = 2e_i \Big/ k_i(k_i - 1) \tag{1}$$

In the formula, k_i is usually expressed as the degree of i-node, and e_i is the number of edges that actually exist between the entrance and its neighbors. The clustering factor C in the network is the root mean square of the clustering coefficients of all nodes, and its expression C can be expressed as:

$$C = \frac{1}{N}\sum\nolimits_{i=1}^{N} C_i \tag{2}$$

In this, N refers to the order of the network.

(2) Average path length

Average path length (APL) is another important feature of the network (Kesari, 2017), which usually refers to the shortest average distance between all pairs of nodes in the network. In this process, the distance between nodes refers to the minimum number of edges that appear from one node to another node, and the maximum distance between all pairs of nodes is called the mesh diameter. Network performance and performance metrics are network diameter and average path length. The formula for calculating the average path length is:

$$APL = \frac{1}{N(N-1)} \sum_{i \neq j \in V} D_{ij} \tag{3}$$

In the formula, D_{ij} is the shortest distance between nodes i and j.

(3) Degree of relevance

Degree correlation is the description of the interconnection between different nodes in the network (Demarco, 2018; Khan, 2016). If higher-order nodes tend to connect to ground nodes, the network is called a positive correlation, otherwise the network is called a negative correlation. Spanish scholars Pastor-Satora, Newman, etc. briefly and intuitively described degree correlation, that is, the calculation of the neighboring average degree of the degree k node, and its value is the correlation function of k. It further simplifies the calculation method of degree correlation, and points out that the correlation degree of the network can only be described by calculating the Pearson correlation coefficient $r(-1 \leq r \leq 1)$ of the peak sequence. The definition of r is as follows:

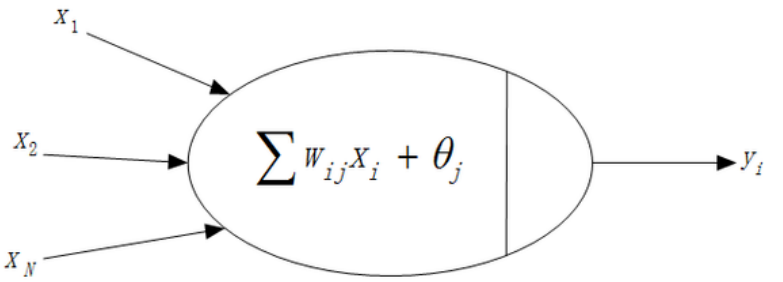
$$r = \frac{M^{-1}\sum_i j_i k_i - \left[M^{-1}\sum_i \frac{1}{2}(j_i + k_i)\right]^2}{M^{-1}\sum_i \frac{1}{2}(j_i^2 + k_i^2) - \left[M^{-1}\sum_i \frac{1}{2}(j_i + k_i)\right]^2} \tag{4}$$

Among them, j_i and k_i each represent the degree of vertices j and k connected to the i-th edge, and M refers to the total number of edges of the network. The value range of r is $-1 \le r \le 1$. In the case of $r > 0$, the network is positively correlated; in the case of $r > 0$, the network is negatively correlated; in the case of $r = 0$, the network is not correlated.

(4) Neural network

The neural network is composed of many simple processing units, which are connected by variable weights to form a parallel distributed system (Berghel, 2017; Kosseff, 2016). The basic processing unit of a neural network is a neuron. Its structure is shown in Figure 1.

Figure 1. General description of neurons



x_i is the input signal, w_{ij} represents the weight of the connection from the i-th neuron to the j-th neuron, and the threshold of the j-th neuron is θ_j. Suppose s_j is the external input signal, y_j is the output signal, the transformation of the jth neuron in the above model can be described as:

$$y_j = f\left(\sum_i w_{ij}x_i - \theta_j + s_j\right) \tag{5}$$

The effect of the u_j processing unit is represented by the output transformation function f_j. If we use $z_j(t)$ to define the u_j output of the neuron at time t, then

$$z_j(t) = f_j(x_j(t)) \tag{6}$$

Or expressed in vector form

$$Z(t) = f(X(t)) \tag{7}$$

Here, $Z(t)$ is on the neural network as the output vector, and f is defined as the state vector and the corresponding function of each component. This function is usually in the interval (0, 1) and is bounded.

(5) BP algorithm

Suppose that there are a total of n nodes and any network of L layers. Each unit of each layer can only receive the information output by the upper layer and output it to each unit of the lower layer. The characteristics of each unit or node are all sigmoid type (Jbb, 2020; Shinde, 2021). To simplify this process, assume that there is only one y output in the network. For N given samples $(x_k, y_k)(k = 1,2,\ldots,N)$, set the output of any node i on the sample as O_i, and for a certain input as x_k, then the network output is y_k, and the output of node i is O_{ik}. When the k sample is input, the node the input of j is

$$net_{ij}^{l} = \sum_{j} w_{ij}^{l} o_{jk}^{l-1} \tag{8}$$

$$o_{jk}^{l} = f\left(net_{jk}^{l}\right) \tag{9}$$

Where o_{jk}^{l-1} represents the 1-1 layer, when the sample k is input, the node output of the j unit is o_{jk}^{l-1}.The error function is as follows

$$E_k = \frac{1}{2}\sum_{l}(y_{lk} - \overline{y}_{lk})^2 \tag{10}$$

Where $\overline{y}_{lk}$ is the actual output of unit j. The total error is:

$$E = \frac{1}{2N}\sum_{k=1}^{N} E_k \tag{11}$$

Definition

$$\delta_{jk}^{l} = \frac{\partial E_k}{\partial net_{jk}^{l}} \tag{12}$$

Then

$$\frac{\partial E_k}{\partial w_{ij}^l} = \frac{\partial E_k}{\partial net_{jk}^l} \frac{\partial net_{jk}^l}{\partial w_{ij}^l} = \frac{\partial E_k}{\partial net_{jk}^l} o_{jk}^{l-1} = \delta_{jk}^l o_{jk}^{l-1} \tag{13}$$

Here, the presentation order of training samples should be randomly generated for each round.

3. OBSERVE THE MAIN MORPHOLOGICAL EXPERIMENTS OF COMPUTER NETWORK CRIME FROM THE PERSPECTIVE OF CRIMINOLOGY

3.1 Crime Scene Investigation

Crime scene investigation is an important part of criminal investigation activities. It is the starting point and foundation of all investigation activities. On-site investigations are of great significance for identifying the nature of the case, analyzing the facts of the case, determining the direction of investigation, delimiting the scope of criminal suspects, and collecting and fixing evidence. Although computer network crimes occur in virtual space, they are the same as traditional criminal cases. After criminals commit computer network crimes, they will also leave traces on the computer system and the Internet. Therefore, when investigating computer network cases, we must attach great importance to the on-site investigation, so as to restore the real scene as much as possible, and lay a solid foundation for the subsequent detection work.

When investigating a specific computer network crime scene, witnesses should be invited to conduct an investigation of the scene. Pay attention to the collection of trace evidence, such as fingerprints and footprints in the room and on the computer, and whether there are some crime-related documents and evidence at the scene. These must be extracted and fixed in a comprehensive and timely manner. Technically demanding is the next search of the computer system. The so-called computer system search refers to an all-round investigation and extraction of computer systems that may contain crime-related data and information by investigators, and a method of obtaining evidence to fix evidence. Before conducting a computer system search, the relevant personnel on the site should be asked about the computer situation, and attention should be paid to the control of the personnel on the site. And taking into account the instability of computer information, there are also features that can be easily operated remotely. If the separation between man and machine is not effective, computer information is likely to be destroyed by man. At the same time, investigators should also pay attention to whether there are strong magnetic wave sources at the computer site and network terminal equipment that may demagnetize the disk data, and remove them quickly if any. In addition, if there is no need for tracking and investigation, try to disconnect the network broadband connection. In some cases, the computer that is implanted with a Trojan horse or becomes a “meat machine” is likely to be controlled by other terminal systems, and data information is tampered with or deleted.

Computer system investigation is mainly to search for traces and evidences of criminal suspects committing crimes. The computer survey should be carried out on the disk that has been backed up in advance to prevent damage to the original evidence. This type of work is now becoming more and more common with the increase in online fraud and other cases. The massive electronic records stored in the server are searched; the key suspicious data is first selected roughly, then finely screened, and then analyzed and extracted based on the recorded information.

3.2 Internet Survey Interview

Investigation visits are routine investigation tools used by criminal investigators to discover the basic situation of a case, find evidence in the case, obtain witness testimony, and verify the credibility of suspicious confessions. Research visit here refers to research visit, especially on the Internet. In traditional cases, investigation visits play an important role in discovering the facts of the case, collecting evidence, and discovering and confirming crimes. This is the most commonly used and

most basic research tool in research work. Computer cybercrime investigations need to learn and use this strategy. The Internet is like a society. The activities of criminal suspects on the Internet are also a social circle and have some understanding of the Internet, such as in communities and chat rooms (Pham, 2019). Searching from these sites is entirely possible. Find useful clues and facts. Internet research interviews are based on this. On the Internet, researchers use QQ groups, chat rooms, forums, and other online instant messaging methods to learn and verify events related to informed Internet users. This opens up another space and also provides another level for research and visits. In addition, the indirect nature of the Internet allows people to communicate more openly in the real world without worry. Compared with visiting the real world, surveys and interviews can provide better clues and evidence. There are several aspects that need to be paid attention to when conducting network survey interviews. Generally speaking, when conducting investigations and visits on the Internet, the investigators first use technical investigation methods to determine the relatively active and frequent places of the criminal suspect, such as forums and chat rooms. After identifying these places, the investigators need to conceal themselves. As an investigator, he entered these places as a general internet user, conducted a thorough investigation of the place, and found and identified key informed internet user. In addition, through online survey visits, you can continue to execute the ongoing plan. Researchers disguised their identity, and all registered IDs were new entrants. Prevent newcomers from trusting surveys and interviews. Therefore, in use, finding the right person among the old internet user can play a multiplier role. Hard work by checking the suspect's QQ space, the suspect can receive a list of friends. Or, you can track people who are in long-term communication in the chat room. Among these employees, find people who are willing to work for public safety services or can be managed and used by public safety services.

3.3 Network Tracking

Network tracking investigation is the use of various software systems or hardware tools to track the location of cybercrimes and specific criminal suspects through a computer network, so that researchers can obtain more information for research methods for obtaining evidence. Network tracking plays a very important role in the investigation of computer network crimes. Because computer network crimes occur in virtual space, the suspect does not appear at the crime scene in a real physical image. We can only determine the crime through the traces of information he left. An effective method is to determine the suspect's possible address based on the electronic information left by the specific online activities of the criminal suspect and set up tracking. Then, when the criminal suspect reappears on the network to perform operations, corresponding measures can be effectively taken. At present, network tracking mainly uses these methods: (1) Tracking based on the IP address of the identified criminal suspect; (2) Tracking through email user name and email address using email header technology.

3.4 Internet Search

Internet search is the search and accumulation of using search engines and other search tools to find criminal information and illegal websites when browsing websites and information on web pages. Internet search can be divided into regular searches to find criminal clues and information. It also includes searching for specific cases, specific criminals, suspects, and evidence.

3.5 Network Waiting

Network waiting refers to a kind of waiting surveillance that investigators need to continue investigating cases or dig deeper in order to expand their results under normal circumstances. In addition, for deeply hidden criminal acts, when all investigative measures have been exhausted and there is no way to identify a criminal suspect, or sufficient evidence for conviction and sentencing cannot be collected, the method of waiting on the spot is used to conduct suspicious sites or accounts. Continuous surveillance is an investigative measure to obtain clues and evidence.

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Types of Computer Cybercrime

Computer network crimes in my country began in the 1980s. According to data records, the first computer crime occurred in 1986. Over the past 30 years, the number of computer network crimes has increased exponentially. In 1986, there were 9 crimes and a sharp increase of more than 2,700 in 2000., There were nearly 30,000 cases in 2005. In addition to these statistics, there are still a large number of unreported cases. Don Parker of the United States estimates that the number of computer cybercrimes is about 80%. According to the latest findings of the US CSI and FBI, only 7% of computer crimes go to law enforcement agencies. In other words, the number of black computer crimes is about 83%. The signs of cybercrime on the computer are different, and the current common cases are cyber fraud, pornography, gambling, etc. Taking a province as an example, according to the statistics of the "Network Case Information System" of the public security system's local area network, from January to May 2017, the province's public security network police departments at all levels opened and assisted in investigating and assisting in the investigation of 580 criminal cases involving the Internet, and solved the cases From 257 cases, various data are shown in Table 1 and Table 2.

Table 1. List of online crime cases in 2017

	Number of online crime cases filed					
	Total	**Obscene**	**Gambling**	**Fraud**	**Theft**	**Other**
Total	580	37	88	329	79	47

By calculating the number of filed computer network crime cases, the rate of filed computer network cases can be obtained, as shown in Figure 2:

Table 2. List of Cases Solved in Internet-related Crimes in 2017

	Number of Internet-related crimes solved					
	Total	**Obscene**	**Gambling**	**Fraud**	**Theft**	**Other**
Total	257	18	54	117	39	29

It can be seen from Figure 2 that fraud, gambling, obscenity, and theft accounted for 81.9% of the total number of computer network crime cases.

From January to May 2019, the province's public security network police departments at all levels jointly filed investigations and assisted in the investigation of various criminal cases involving the Internet. It is found that computer network crime cases have further increased, with the total number of cases reaching 1,462, and 741 cases solved. Various data are shown in Table 3 and Table 4.

Figure 2.

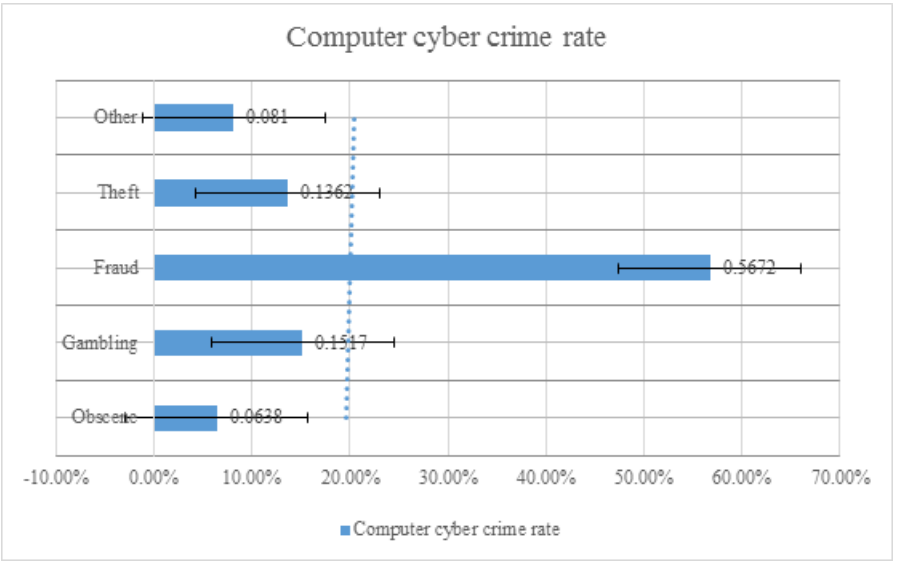


Table 3. List of online crime cases in 2019

	Number of online crime cases filed					
	Total	Obscene	Gambling	Fraud	Theft	Other
Total	1462	107	213	780	204	158

Table 4. Cases Solving List of Internet-related Crimes in 2019

	Number of Internet-related crimes solved					
	Total	Obscene	Gambling	Fraud	Theft	Other
Total	741	61	99	392	112	77

4.2 Age Level of Computer Cybercrime

In 2017, the province's public security network police departments at all levels filed and assisted in investigating and assisting in the investigation of 580 online criminal cases for each age group. Figure 4 can be obtained.

In 2019, the province's public security and cyber police departments at all levels filed investigations and assisted in the investigation of 1,462 criminal cases involving cybercriminals for each age group. Figure 5 is available.

As can be seen from Figures 4 and 5, among various computer cybercrimes, the 20-35 age group accounts for a relatively large number of people, and the proportion of people under 35 who commit computer cybercrimes is relatively high. In 2017, various cases among them, the proportion

Figure 3. Comparison of the rate of various computer network crime cases in two years

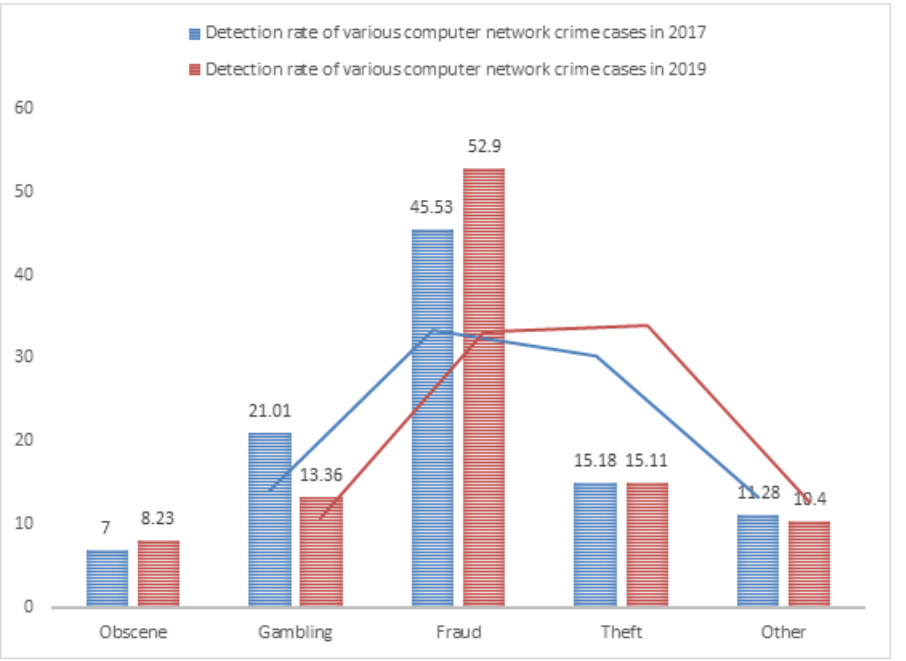


Figure 4. Statistics of various age groups in various computer network crime cases in 2017

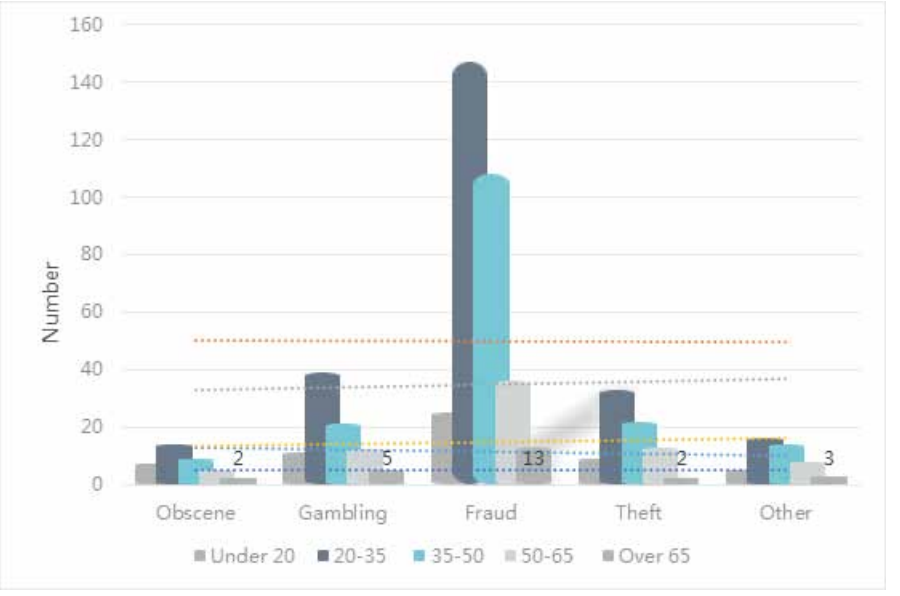
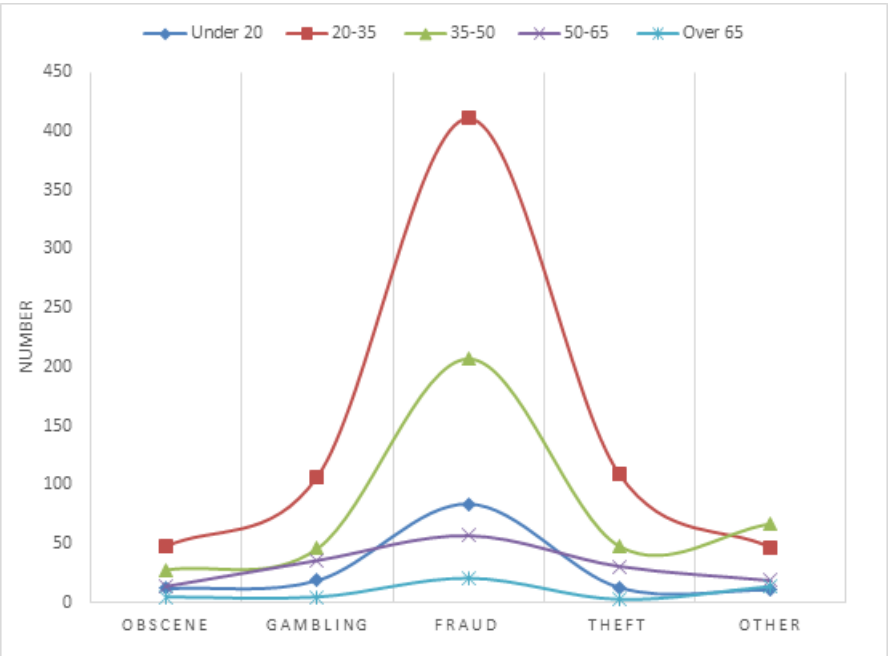


Figure 5. Statistics of various age groups in various computer network crime cases in 2019



of criminals under the age of 35 accounted for 52.76% of the total, and the proportion of criminals under the age of 35 in various cases in 2019 was as high as 58.89%.

According to the types of computer network crimes and the age level of computer network crimes, it can be found that among various computer network crimes, the proportion of fraudulent and computer network crimes committed by people under 35 is relatively high.

5. CONCLUSIONS

Computer network has been popular in China for about 10 years. With the continuous development, it has penetrated into every corner of daily life and become an important way of people's life. In this era of complex information, the forms of crime are so diverse and complex. With the development of science and technology, computer network crime will take on more complex forms, and the harm to society will be more serious. Therefore, it is urgent to enrich and develop the ideas and measures of computer network crime investigation from the concept and practice, so as to serve the investigation practice and improve the investigation effect. The arrival of the era of big data gives us the opportunity to combat and prevent such crimes. In the big data environment, all Traces of human behavior will be recorded in a panoramic way; Terrorists are no exception to the massive data in the network. The efficient combination with cloud computing can provide strong support for preventing and combating the crime of cyber terrorism. How to build an anti cyber terrorism system around big data and maintain the security and stability of China's cyberspace sovereignty will be an important issueIt is a research focus of anti-terrorism work in the past and in the future. This article combines big data with cyber terrorism. It not only analyzes the current situation of big data security management in the prevention and control of computer cyber crimes, but also analyzes the characteristics of computer cyber crimes and discusses them in the process of studying computer cyber crimes. The big data security management countermeasures in the prevention and control of computer network crimes. It closely connects with the reality and probes into the computer network crime under the new situation.

We should reasonably and scientifically construct the investigation mechanism of network crime, and put forward practical and effective investigation measures. Due to the limitation of knowledge, many views may not be rigorous. Computer cybercrime is a subject worthy of in-depth and long-term research. I hope this article can serve as a reference.

REFERENCES

Aaron, H. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, *2018*(7), 13–15. doi:10.1016/S1361-3723(18)30064-2

Berghel, H. (2017). Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election. *Computer*, *50*(9), 87–91. doi:10.1109/MC.2017.3571054

Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. *Computer Fraud & Security*, *2018*(11), 8–10. doi:10.1016/S1361-3723(18)30108-8

Demarco, J. V. (2018). An approach to minimizing legal and reputational risk in Red Team hacking exercises. *Computer Law & Security Review*, *34*(4), 908–911. doi:10.1016/j.clsr.2018.05.033

Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer Law & Security Report*, *33*(5), 700–717. doi:10.1016/j.clsr.2017.03.020

Gao, L., Liu, L., & Feng, Y. (2017). Factors Affecting Individual Level ERP Assimilation in a Social Network Perspective: A Multi-Case Stuty. *Journal of Global Information Management*, *25*(3), 21–39. doi:10.4018/JGIM.2017070102

Hardik, Runwal, & Pooja. (2018). A Survey on: Cyber Crime & Information Security. *IOSR Journal of Computer Engineering*, *20*(1), 30–34.

Hert, P. D., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Security Report*, *34*(2), 327–336. doi:10.1016/j.clsr.2018.01.003

Hinchliffe, A. (2017). Nigerian princes to kings of malware: The next evolution in Nigerian cybercrime. *Computer Fraud & Security*, *2017*(5), 5–9. doi:10.1016/S1361-3723(17)30040-4

Jbb, . (2020). ARIES: Evaluation of a reliable and privacy-preserving European identity management framework - ScienceDirect. *Future Generation Computer Systems*, *102*(C), 409–425.

Kesari, A., Hoofnagle, C., & Mccoy, D. (2017). Deterring Cybercrime: Focus on Intermediaries. *Berkeley Technology Law Journal*, *32*(3), 1093–1133.

Khan, S., Gani, A., Wahab, A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications*, *66*(may), 214–235. doi:10.1016/j.jnca.2016.03.005

Kosseff, J. (2016). The hazards of cyber-vigilantism. *Computer Law & Security Review the International Journal of Technology Law & Practice*, *32*(4), 642–649. doi:10.1016/j.clsr.2016.05.008

Kouttis, S. (2016). Improving security knowledge, skills and safety. *Computer Fraud & Security*, *2016*(4), 12–14. doi:10.1016/S1361-3723(16)30037-9

Laviero, B. (2016). Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. *ERA Forum, 17*(3), 343–353.

Lee, L. (2019). Cybercrime has evolved: It's time cyber security did too. *Computer Fraud & Security*, *2019*(6), 8–11. doi:10.1016/S1361-3723(19)30063-6

Li, J. (2017). Investigation Tools for Cybercrime. *Advances in Computational Sciences and Technology, 10*(12), 3263-3276.

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14–17. doi:10.1016/S1361-3723(20)30019-1

Lux, L. M. (2017). The object of legal protection in cybercrimes. *Revista Chilena de Derecho*, *44*(1), 235–260.

Maher, D. (2017). Can artificial intelligence help in the war on cybercrime? *Computer Fraud & Security*, *2017*(8), 7–9. doi:10.1016/S1361-3723(17)30069-6

Mazurczyk, W., Holt, T., & Szczypiorski, K. (2016). ' Introduction: Special Issue on Cyber Crime. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 146–147. doi:10.1109/TDSC.2015.2502407

Namasudra, S., & Roy, P. (2018). Ppbac: Popularity Based Access Control Model for Cloud Computing. *Journal of Organizational and End User Computing, 30*(4), 14-31.

Orji, U. J. (2019). A Review of the ECOWAS Cybercrime Directive. *Computer Law Review International*, *20*(2), 40–53. doi:10.9785/cri-2019-200204

Parada, R., Melia-Segui, J., & Pous, R. (2018). Anomaly Detection Using Rfid-Based Information Management in an Iot Context. *Journal of Organizational and End User Computing, 30*(3), 1-23.

Parah, S. A., Sheikh, J. A., Dey, N., & Bhat, G. M. (2017). Realization of a New Robust and Secure Watermarking Technique Using DC Coefficient Modification in Pixel Domain and Chaotic Encryption. *Journal of Global Information Management*, *25*(4), 80–102. doi:10.4018/JGIM.2017100106

Pham, L. M. T., Tran, L. T. T., Thipwong, P., & Huang, W. T. (2019). Dynamic Capability and Organizational Performance: Is Social Networking Site a Missing Link? *Journal of Organizational and End User Computing*, *31*(2), 1–21. doi:10.4018/JOEUC.2019040101

Poltavtseva, M. A., Zegzhda, D. P., & Kalinin, M. O. (2019). Big Data Management System Security Threat Model. *Automatic Control and Computer Sciences*, *53*(8), 903–913. doi:10.3103/S0146411619080261

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy and Research*, *22*(1), 1–25. doi:10.1007/s10610-015-9277-7

Richardson, J. (2020). Is there a silver bullet to stop cybercrime? *Computer Fraud & Security*, *2020*(5), 6–8. doi:10.1016/S1361-3723(20)30050-6

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. doi:10.1109/TDSC.2015.2410795

Rock, A. (2017). Cybercrime gets personal. *Money*, *46*(2), 66–74.

Shinde, N., & Kulkarni, D. (2021). Cyber incident response and planning: A flexible approach. *Computer Fraud & Security*, *2021*(1), 14–19. doi:10.1016/S1361-3723(21)00009-9

Singh, A., & Kaur, M. (2020). Detection Framework for Content-Based Cybercrime in Online Social Networks Using Metaheuristic Approach. *Arabian Journal for Science and Engineering*, *45*(4), 2705–2719. doi:10.1007/s13369-019-04125-w

Stearns, B. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments - ScienceDirect. *Computer Law & Security Review*, *34*(6), 1180–1196. doi:10.1016/j.clsr.2018.08.005

Xie, P. S., Fan, H. J., & Feng, T. (2020). Adaptive Access Control Model of Vehicular Network Big Data Based on XACML and Security Risk. *International Journal of Network Security*, *22*(2), 347–357.