Critical Inforamtion Detection for the Prevention and Control of Burst Cybercrime Events under the Background of Big Data

Cheng-De Zhang, Yan-Peng Pan
School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan, P.R. China
E-mail: chengdezhang@znufe.edu.cn, yanpengpanx@gmail.com

***Abstract*-With the popularity of computer and internet, cybercrime is rampant. However, the characteristics of internet making it more difficult to monitor the cybercrime, such as openness anonymity high speed and across localization. In this paper, we propose a new method to prevent cybercrime. Critical Information are taken as important information to monitor burst cybercrime events in massive data. With the detection of characters about critical people and information, we can quickly discover the network crime, and then the government can intervene in time. Therefore, this method can reduce the harm of cybercrime, and the loss of state.**

Keywords-big data, cybercrime, burst event, prevention and control

I. INTRODUCTION

After 9.11 terrorist attack, international anti-terrorism situation entered a new historical stage, the popularity of internet technology makes terrorism globalism. "East Turkistan" terrorist incited and planned a series of violent terrorist attacks in Sinkiang, Beijing, kunming and other places. China is now in a state of high incidence of terrorist attacks, anti-terrorism situation is very serious, violent and horrible crime has been growing concerned. East Turkistan terrorists often spread violent terrorist audio and video through internet to confuse the messes to participate in Jihad. In order to resist and fight cyber terroristic criminals and strengthen international cooperation, it is urgent to make a deep research about the prevention and control of butst cybercrime event in China.

Since the end of last century, mankind ushered information age. The number of cybercrime shows explosive growth, while people enjoy the convenience of the internet.

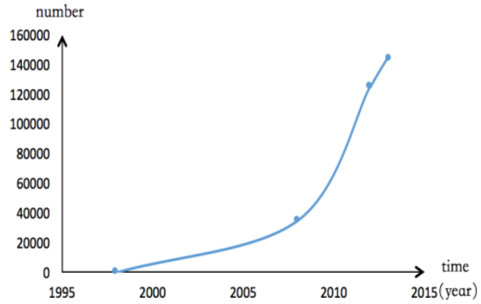

Figure 1. The number of cybercrime handled by Chinese public security department.

As shown in Figure 1, the number of cybercrime handled by Chinese public security department grows exponentially, from 1998 to 2013. In 2013, the number of Chinas cybercrime reached 144 thousand. Compared with traditional crime, cybercrime is more harmful, destructive and durable. It is urgent for the research of monitoring the burst cybercrime event.

As involving multiple subjects, multi-disciplinary cross research is inevitable.

A. Legal Aspects

In the study of law, Chinese internet security act is far from perfect. Because the late initiation of research of Chinese Internet security act. In the early stages of the development of the internet, Chinese emphasis on internet security and the provision of cross-border crime is not enough. For example, under the penal code of China, This Law may be applicable to any foreigners who commit a crime outside the territory and territorial waters and space of the People's Republic of China against the State of the People's Republic of China or against any of its citizens, if for that crime this Law prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, this does not apply to a crime that is not punishable according to the laws of the place where it is committed. Although Chinas foreign cybercrime is rampant, present law cant effectively solve the cybercrime problem which is high concealment and not geographical Limited. The Ministry said: ninety percent of bilk websitephishing website and gambling website aimed to Chinese Internet users locate their server outside china, transnational cooperation to fight cyber crime is urgent. There are many mature legislative model overseas, such as Special legislation model (American)Government regulation and industry oversight combined legislation model(England), The legislative model of the combination of government regulation and industry supervision (Japan), prudential supervision and legal prevention and control mode (Germany) [1-3]. However, due to the different national conditions, we can not copy foreign legislative model. It is urgent to find a legislative model especially designed for China. As society growsincreasinglyconcernedover internet security, many scholars have made suggestions on the cybercrime security legislation. Such as professor Xu Hanming proposed that Chinese legislation should strengthen the supervision of the government and make government the leading role in the multi-governance [3]. Monitoring and prevention of cybercrime necessarily need to monitor the data in the Internet, which has a certain conflict with privacy, but due to the importance of Internet security, we must insist on the principle that Security First, but freedom is also important [4]. About the international cybercrime, we can also try to establish a International permanent mechanism to combat it [5].

Compared with the traditional information, the network information disseminates faster and has the bigger data quantity so it is more difficult to monitor. For some reason, most Chinese people have conformist mentality, but few dare to question. So the false information is easy to form The Spiral of Silence [6] under the guidance of some criminals. Chances are high that a lie will be accepted as truth in China when its repeated often, especially in the virtual environment like Internet which is hard to distinguish between truths and lies. So it is very necessary to study the prevention and control of false information.

B. *Computer-Related*

When the Internet has just entered China, China had the small and slow network communication and flimsy network information. Illegal invasion of computer systems and spread of the virus is a popular means of cybercrime. But with the progress of science and technology and the arrival of the era of Big Data, the importance of information has become increasingly prominent, the subject of cybercrime is slowly changing from computer hardware to the data and information spread on the internet [7-10]. Traditional detection methods is facing enormous challenges, while the cybercrime in China presents some new features.

- Low-cast: duo to the popularity of computer, cybercrime just need a personal computer connected to the Internet, and the cost has been far lower than the traditional crime. This will increase the universality of cybercrime.
- Across localization: As computer network is a global World Wide Web. Cybercriminal could commit cybercrime at home. This character makes traditional monitoring method difficult to work.
- Instantaneity: The information is the rapid transmission on the Internet. If we can detect the cybercrime and promptly stop it, we will cut down the country and people loss to minimum.
- High concealment: Network user is virtual and everybody could have many virtual identity, which increases the difficulty of hunting and detecting cybercrime and objectively provides a breeding ground for the development of cybercrime.
- High harmfulness: with the advent of the"Internet plus" era, not only service industry, tourism, sports and cultural industry, but also the industry which involves national and social stability like finance, petroleum, politics and telecom had slowly integrated into the Internet plus. As a result, the influence of Internet will increase in proportion to Internet plus, so do the influence scope and harm of cybercrime.
- High-technological: compared with the traditional criminals, the cybercriminals have higher educational history, more knowledge reserve and more economic foundation .So they are more harmful. They may even be spies that assigned by other countries to subvert the regime and destroy the stability of our country.

China's cybercrime monitoring in the law and computer are both facing new challenges. Neither of them could solve it perfectly. The only way to eliminate cybercrime fundamentally is to make full use of computer technology to detect cybercrime and to develop appropriate laws and regulation and corresponding sanctions.

II. CRITICAL INFORAMTION PREVENTION AND CONTROL

A. *Judicial Prevention and Control*

In terms of legislation, China's Internet Security legislation should be based on the national conditions in China, refer to the advantages of other countries properly and insist on governing the country by law. Then network security laws especially suitable for China can be proposed. Moreover, Chinas legislation related to cybercrime are supposed to pay special attention to clear the criminal subject and refine the crime types. For example, now it is a quite obvious tendency that adolescents commit cyber crimes at their younger age. If we have not cleared the criminal subject, they might escape from law punishment.

In the field of law enforcement, we should ensure to enforce the law strictly and punish all offenders in order to avoid the Internet Security Act existing in name only. Only in this way can dispel the criminals fluke mind and establish the majesty of the Internet Security Act.

B. *Moral Restraint*

Morality and law are important means to restrict people's behavior and maintain social order. But the law is rigorous, so it cant cover all social phenomenas and update timely according to the change of criminal methods. Therefore, we can only restrict peoples behaviors by moral when laws cant make it. We all know that China remains a developing country, national quality and ethical standards are in low-level, which makes it very important to improve the influence of moral restraint because of the insufficient coverage of the Internet Security Act . China should increase the publicity for the prevention and control of cybercrime and emphasize theillegalityof cybercrime in order to make people fully realize that the cybercrime is illegal as well as the traditional crime. In addition, government should also fully cultivate people's enthusiasm and make them resist cybercrime spontaneously so that the cybercrime would have nowhere to hide like a rat crossing the street.

C. *Social Prevention and Control*

Generally speaking, in the process of spreading rumors, the few parts of the criminals create rumors and send it to the Internet, then unwitting masses help them spread it. The reason why the masses will help criminals to spread false rumors is mainly that the credibility of the government and mainstream media is not enough. The role of the media is to pass real information to the masses, but in order to improve the click rate and browse quantity, some web-media write an attractive title and some even spread unconfirmed rumors. In this case, people without the exact information sources, they cannot clearly distinguish between facts and rumors, they can only spread information they willing to believe. Thats why the rumor is widespread.

Network rumors spread is lacking of monitoring, thus the social prevention and control tasks has a long way to go, especially for mainstream media and government. When the mainstream media and the government have a very high credibility, even though the rumors appear, so long as government clarify in time, rumors will collapse without being attacked.

D. Technology Prevent and Control

Because of the network information sharing, network information dissemination is usually in exponential growth. We can suppose that each transmitter transfers 100 or 10 people in the Internet. Mathematical formulas can be expressed as:

$$y_1 = 100^x \tag{1}$$

$$y_2 = 10^x \tag{2}$$

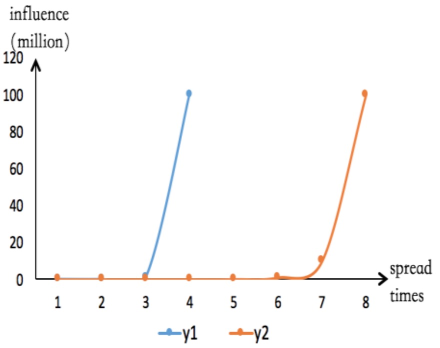

Figure 2. The situation of influence with different times about propagation

In those two mathematical formulas, argument x is the number of information dissemination, y1 is the information impact curve while each transmitter transfers 100 people once and y2 is the information impact curve while each transmitter transfers 10 people once. Figure 2 shows the soar of influence while the number of transmissions increasing slowly.

It can be infered from Figure 2 that the rumors influence will dramatically increase if each transmitter transfers 100 people each time. While each transmitter transfers 10 people each time, the influence of rumor would also explosive growth after being spreaded 7 times. According to the 8-2 rule proposed by Vilfredo Pareto, we should pay more attention to the top 20 percent people.

In a word, information growth curve has an explosive point. This explosive point is the key point in information security prevention and control. If we can find out and filter social harmful information, then we could reduce the influence of information to the lowest level, or there might be too much data.

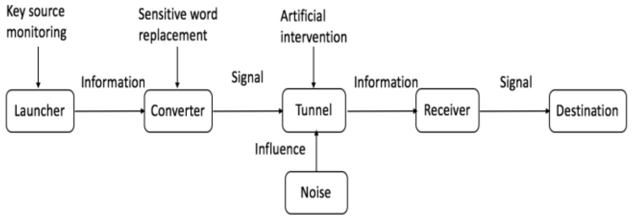

Figure 3. Advanced Shannon - Weaver mathematical models.

According to Figure 3 Shannon-Weaver mathematical models, Information dissemination has five essential factors: information source, launcher, channel, receiver, destination and an influential factorsnoise. Because the destination, launcher and receiver are difficult to change, so we can focus on three critical information: information source, channel and noise. Combine Shannon - Weaver mathematical models and impact curve, we can find the main factors that determine the influence of network information are the influence of information disseminators, the number of information dissemination and noise, so we should focus on those three key points:

- Critical persons: The critical persons should be closely monitored, such as the twitter users attended by tens of thousands. The information released by them are easy to cause great repercussions, because they have grate influence, more fans and more information sources. By monitoring the key persons, we can greatly reduce the monitoring burden and improve the monitoring efficiency. By extracting keywords published by key figures, making semantic analysis and detecting the similarity of sensitive words or pictures, it would be easier to find information involving cybercrime or influencing social stability. Moreover, it would be reduce reduce the social losses.
- Key information dissemination: When the cybercrime incident happened, the information flow of keyword and sensitive image would rapidly expanding in a short time. By extracting and analyzing the key information flow volume growth curve of the change, cybecrime would be detected in the early of bursty events spreading. Then we can accuratly locate information sources, promptly cut off the diffusion path of the information, and minimize harms to society.
- Effects of noise: As extrinsic factors would influence the propagation of information. In order to effectively reduce the harm cybercrime information, Upon detection of crime information has not been

able to prevent its spread and source tracing, we can use information antagonistic approach to publish attractive news to resistance spread fake crime messages.

III. CONCLUSION

With the continuous progress of internet technology, more and more cybercrime incidents occurred. This paper proposed a new method for cybercrime prevention and control. Based on network information technology, both law and computer science knowledge are considered for effectively grasp the principal information to improve monitoring efficiency. In the future, we will focus on source tracing and clean-up about cybercrime information to further improve the efficiency of prevention and control.

ACKNOWLEDGMENT

This work was supported by MOE (Ministry of Education in China) Project of Humanities and Social Sciences (Project No. 16YJC860026).

REFERENCES

[1] B. Zhou, Cybercrime is increase under the high pressure, criminal channels become more and more mature, Legal Daily, 2014 , pp: 1-2.

[2] J. Song, Study of the cybercrime criminal legislative Defects and Perfect in our country, A Dissertation Submitted to the Graduate School of Henan University in Partial Fulfillment of the Requirements for the Degree of Master of Law, 2013, pp: 13-18.

[3] H. Xu, L. Zhang, Reflections over the Prevention and Punishment of Online Financial Crimes in the Big Data Era. Comparative Economic & Social systems, No.3 2015, pp:13-14

[4] H. Xu, Network Governance: Security Efficiency First and Consideration to freedom, Chinese Social Sciences Weekly, 2014, pp: 1-2.

[5] Z. Xu, On Network Crime and Its Prevention, Master's degree thesis of Jilin University, 2005, pp: 50-51.

[6] Noelle-Neumann, Die Schweigespirale, 2013.

[7] Viktor Mayer-Schnberge, Big Data: A Revolution That Will Transform How We Live, Work, and Think, 2013.

[8] S. Liu, X. Sun.: Crime on Internet, JOURNAL OF PEKING UNIVERSITY Humanities and Social Sciences, 2001,38(3) , pp: 115-116.

[9] Y. Guo, X. lv, Z. Li, Bursty topics detection approach on Chinese microblog based on burst words clustering, Journal of Computer Applications, 2014,34(2), pp: 1-6.

[10] W. Li, Z. Yu, J. Gong, R. Chen, An Approach of Crime Network Analysis Based on Association Data Model. ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS SUNYATSENI, 2014, 53(5), pp: 1-7.