ATLANTIS PRESS

Advances in Engineering, volume 100

International Conference on Manufacturing Engineering and Intelligent Materials (ICMEIM 2017)

Hidden Danger and Protection Strategy of Cyber Security

Guan-ying Yang

School of Law, Henan University of Technology, Zhengzhou,

ygyemail@163.com

Keywords: Website Capture, Digital Evidence, Cyber-Crime, Law Enforcement

Abstract: With the Internet emergence in the recent decade, not only is the E-commerce promoted, but also cyber crime is posed accordingly. Due to the properties of anonymity, no boundary, and fast propagation on Internet world, it is more difficult for the law enforcement members to seize the suspects who engage in the illegal behavior. In response to the Internet security problems, in this paper, an in-depth study of major security threats are made and some suggestions have been built for the computer crime detection. The proposed measures included the organization, training, technical capability, legislation and operation procedures. It is expected that hidden danger will greatly reduce to cyber security policy and management in the future by using the measures.

Introduction

A computer is the source of evidence and an eyewitness to any crime related to cyber space or computer system. Fortunately, the evidence is secretly stored in it. Forensic analysis of a computer would uncover the evidence related to a crime. Computers, networks and Internet provide new capabilities and opportunities for users and businesses to interconnect, access information, and execute (a new range of) activities in a fast and easy way. Unfortunately, these new capabilities and opportunities are also available for criminals to carry out their illegal activities. Not only do computers and networks serve as an accelerator for existing types of crime, they enable new types of crime as well. In practice cybercrime is committed by individuals or small groups (disorganized crime), as well as by criminal groups (organized crime). Cybercrime, which impacts individuals, public and private organizations alike, has become a rising concern of nations in this golden era of Internet and cyberspace.

For the safe operation of combat cyber crime, the protection of the Internet, our decision on safeguarding Internet security, issued November 20 2006. Explicitly in the document （Classified criteria for security）of China, to be held criminally responsible Internet behavior which constitutes is a crime. Which the decision first sets out the following acts, including acts of intentionally spreading computer viruses and other destructive programs, attacks on computer systems and communication networks, resulting in computer systems and communication networks suffer damage, in violation of state regulations, unauthorized interruption of computer network or communication service, resulting in the behavior of computer networks or communications systems may not run. In Sec.1 explicitly refers to the following acts, `including the illegal interception, tampering, delete others 'e-mail or other data behavior, violation of the behavior of the citizens' freedom and privacy of correspondence, use the Internet for theft, fraud, extortion behavior.

The author also points out a number of the mismatches that exist between, on the one side, rising cybercrime threats and, on the other side, the existing tools (i.e., information security systems) and rules (laws and legislations). Ultimately, our objective is to identify and outline a number of research directions in legislation, social and technical arenas that boost the role of users and organizations in combat against cybercrime.

A war against cybercrime in a democratic society is impossible unless there are clear definitions of such crimes and appropriate laws and governance mechanisms to safeguard the rights of all parties. Statistics on the frequency of computer/Internet crimes point to the value of the enactment of computer crime-specific laws and illustrate how computer crime has moved towards the front of

crime concerns for the nation. In recent times, cyber-crime is considered to be the world's biggest growth industry. The impact of digital advances has changed the landscape of the crime scene, amplifying further the need for cross-boundary collaboration, revised sound forensic practices and surrounding procedures. Technology is advancing so rapidly that few people ever realize the complexity. The menace of organized crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy electronic and security systems develops.

Cyber Crime Faces New Problems and Reflections

The author believes that many criminal acts on the Penal Code provisions on computer and network crime in the identified lack of Elements, the lack of actual operability facing some new problems.

An Object of a Crime is not Clear

(1) Ruler of Protection and Property Rights Provisions are not Clear

Property or money on the Internet, the property is not in the traditional sense, but the form of virtual currency, virtual property. "Q coins" network virtual property is not property? A firmed in judicial practice. A company leaving the employees where Wang (due to suspended sentences with a pseudonym) theft boss in the online Q coins, the District Prosecutor's Office to prosecute, the district court finds that the employee's conduct constituted theft, recently sentenced to prison for six months, suspended for 1 year and fined 1,000 Yuan. A CD (Compact Disk) with an e-learning application is such a product, because the CD itself is a physical object, while the content is a digital product. It is unclear how the law deals with crime committed on these objects. Recently, the High Court has stated that the theft of an avatar is actionable, since the creation of the avatar requires a significant amount of time and effort. The judge held that the game equipment, and other virtual property is the friends in the course of the game, invest time, energy, personal intelligence and even money, also has the properties of general merchandise, and its true value should be protected by law. So, as long as the virtual property theft of valuable, able to exchange money, all constitute theft.

(2) Violations of Intellectual Property are Difficult.

Information on the Internet and publishing division is not clear. The exchange of multimedia works is attributable to the publication and distribution? The regular publication of a work usually in the form of books, periodicals, newspapers, audio-visual products must have a formal ISBN and publishing license, otherwise you can treat the illegal publication of acts. But on the Internet, and no national boundaries and the police, anyone can feel free to publish their own or others' works. This behavior may not be for commercial purposes, at the same time to see this information free to copy these works and does not require any formalities.

Therefore lead to the judicial practice will find some of the issues, the legal principles to determine whether this behavior is illegal, and who will determine whether an offense has become the problem in the judicial practice.

The Behavior of the Objective Aspect of Crime is Unknown.

The crime of computer theft, a common Italian sausage surgery this crime is not easy to make the victim aware of the ways in which the victim unconscious to make minor concessions to the interests, add up in order to achieve a criminal purpose. For example, as a hacker, Zhang online purchased credit card numbers, bank account information and personal information of cardholders. Taking advantage of the loopholes in the online banking settings, and using brute force password cracking, Zhang could easily set the certificate password and then download the certificate. With the system vulnerability in the certificate security, he could successfully break through the certification process and then steal money from the accounts. Using the tool software downloaded from the Internet, he cracked the password of the wireless AP in the neighborhood and accessed the Internet to use the

credit cards of others with the spillover of someone else's wireless network, with his online record hidden. A small amount, is often difficult to immediately find the program to run automatically, so no obvious criminal act. We are usually talking about computer and network fraud or fraud, always the consequences of criminal behavior or taken by the Trojans implantation means to do empirical judgment.

Criminal Jurisdiction is not Clear.

"Virtual world" of criminal procedural law governing space and scope of the challenge is a comprehensive, multilevel, not in advance to strengthen the countermeasures research and professional preparation, and will inevitably cause a certain period of time or a certain degree of criminal jurisdiction gap, its the impact of the Criminal Procedure Law jurisdiction is evident. Further challenges with investigation arise when crimes are committed across borders which invariably are the case.

Many commentators have alluded to the challenges facing across border investigations. Across border crime commission affects many jurisdictions and in respect of law enforcement co-operation, issues such as sovereignty and dual criminality to name but a few, may become stumbling blocks. As a result there is an urgent need for harmonization of laws in respect of cybercrime prevention, detection, investigation and prosecution. This ultimately results in the question as to which body will ensure such harmonization of cybercrime laws? The only treaty at present that may be used as a guideline for such harmonization of laws is the Council of Europe (COE) Convention of Cybercrime (Cybercrime Convention) of 2001. Although the issue of harmonization will be discussed hereafter, it is important to note that harmonization has not yet been affected.

Unlike physical crime, cybercrime may be committed from a country without the physical presence of the accused. The much coined quote "justice is only done if it is seen done" is very relevant when it comes to prosecution. Unfortunately, even where the accused is identified, a request for extradition of the accused from the country where the crime originates and most probably the country of which the accused is a citizen and the country where the effect of the crime is felt, may be contentious and have diplomatic repercussions. The latter may be avoided by looking at the application of issues of subjective territoriality and objective territoriality in respect of cybercrime. In terms of subjective territoriality the country of origin may prosecute the accused citizen whereas in terms of objective territoriality the country where the effect was felt may insist on prosecution. The latter is illustrated with reference to the extradition request in 2012 by the United States of America (US) to the Russia for the extradition of a US citizen, Snowden, who to listen in on a stream for events country military between February 2001 and March 2012. Although the US has requested the extradition of Snowden in terms of objective territoriality, he has not as yet been extradited due to various legal objections. Most national security strategies converge on the notion that the state traditionally is responsible for the security, safety, and well-being of its citizens. Particularly within military affairs, states claim the prerogative of creating and judging political legitimacy. National policies, mentalities and considerations regarding sovereignty in jurisdictional powers of the individual state remains pivotal in maintaining state monopoly of the use of force and questions traditionally related to national security.

On cybercrime jurisdiction, academia has the following theory: the theory of relative jurisdiction, the web site under the jurisdiction of theory and territorial jurisdiction of the theory. These theories in practice are reasonable, but relatively speaking, also have shortcomings.

The Impact of the Traditional Criminal Law Offenses and Types of Online .

Criminal acts are punishable by law, but a great number of offences are prosecuted by the use of the 'classic legislation' to regulate, for example, child pornography, theft, abuse, and similar acts. Free pirated software, hacker programs, Trojans, feel free to download, there is no way to monitor the use of although the software is obvious with the harm to society, but in judicial practice, for the qualified majority of instruments of crime, yet the exact requirements. Our criminal justice system is mainly focused on physical objects. However, computers and networks entail also virtual and hybrid objects,

on which crime may be committed. For example, an avatar, which is a virtual object, can be stolen or destroyed. This also holds for hybrid products. A CD (Compact Disk) with an e-learning application is such a product, because the CD itself is a physical object, while the content is a digital product. It is unclear how the law deals with crime committed on these objects.

Insufficient Evidence of the Type of Computer Crime .

Appropriate increase in the types of criminal evidence, improve the evidence system. Computer-stored data should be regarded as the audio-visual materials, just the technical nature of these data, especially non-professionals also difficult to identify, it is difficult to get recognized by the court. As a foreign expert pointed out: “Not only in Britain but also throughout Europe and the United States, even the prosecution of the smallest fraud, computer-related evidence is difficult to be recognized.” Due to network forensics focuses on finding out the truth of illegal or criminal activities from evidences, therefore we need to explore digital forensics process and regard it as the procedure of network forensics basis.

According to the digital forensics process, the first Digital Forensics Research Workshop produced seven steps of process are: (1) Identification, (2) Preservation, (3) Collection, (4) Examination, (5) Analysis, (6) Presentation, and (7) Decision. And proposed a framework includes nine components are: (1) Identification, (2) Preparation, (3) Approach strategy, (4) Preservation, (5) Collection, (6) Examination, (7) Analysis, (8) Presentation, and (9) Returning evidence. Proposed forensics process consists of four phases are: (1) Collection, (2) Examination, (3) Analysis, (4) Reporting. From the views above mentioned, we summarize the process should be fully prepared before forensic work over the original digital evidence acquisition, analysis of the results should take appropriate protective measures, forensic history is necessary to record the steps, and the final forensic report must be output to show findings of network incident with cybercrime relationship.

On Cybercrime Laws And Governance

The New Requirements of The Traditional Subject of Crime.

In business, some companies in order to win in the field of commercial competition, or for the protection of their own intellectual property rights of purposes, and to take the network means to limit and even undermine each other's computers and networks, users and competitors piracy. 1997, Beijing has undergone a similar event. An anti-virus software company anti-virus software to its products of a particular model “logic lock” to prevent being pirated, so that the computer installed the software does not work properly.

However, the main body of the crime of invasive calculation of the information system in the provisions of section 452, 285, 286,287 of the Criminal Law, crime and destruction of computer information systems does not contain units. This author believes that it is necessary to the unit main body into the scope of computer crime regulation.

Nowadays we regularly hear about law enforcement authorities exercising and improving their cybercrime monitoring activities. For example, the Energy and Commerce Committee of the US House of Representatives has recently asked Apple Inc. to explain about the company's efforts to protect the privacy and security of its mobile device users. The committee is concerned about the way that apps access photographs on Apple mobile devices and the tools for consumers to prevent unwanted online tracking. As another example, the U.S. Federal Bureau of Investigation (FBI) currently looks for a tool to gather and mine data from blogs and social networks such as Facebook and Twitter. The FBI objective is to know about breaking events, incidents and emerging threats. The FBI wants to use the system only to monitor publicly available information and not to focus on specific individuals or groups. Nevertheless, such measures raise the concerns of privacy protection activists.

Judicial authorities have issued a number of important verdicts against cybercriminals recently. The US department of Justice website enlists a number of such verdicts over a wide range of

cybercrimes, for example: denial of service attacks, illegal computer monitoring, botnet computer tampering, bank and credit card fraud, illegal download, production and sell of copyright materials, and stealing the Internet service. Issuing such judicial verdicts demonstrates the determination of the justice system to deal with cybercrimes. There are also judicial actions against ongoing practices of application service providers that pave the way for misuse and crime. For example, the Friend Finder feature of Facebook allows users (even those who are not Facebook members) to input the e-mail addresses of others to the site. Then Facebook uses these address lists and invites their owners to the network. A court in Berlin has recently ruled that this practice of Facebook is unlawful in Germany. It is expected that this court's rule will be followed in other countries. Nevertheless, there is quite a delay between rolling out such debatable functionalities and legal actions against them.

Precaution Mechanism of Computer Emergency

(1) National cyber forensic standard of operation and assessment: Development of National standard of operation of cyber forensic is critical to the overall advancement of it.

(2) Automation network mining system regarding cyber crime investigation: To develop automation network mining system to reduce human involvement in routine, and to utilize artificial intelligence technology to make it more effectively in prevention of cyber crime.

(3) Artificial Intelligence trap system- Learn, adapt, and evolve: Present trap system is under academic research, we aim to incorporate it with Al system to reduce error and equip with the ability to learn, adapt, and evolve to reinforce effectiveness.

(4) Network intrusion and detection laboratory with arbitration system: To conduct the research of network intrusion and detection laboratory for Network security, and also design an environment control system to precisely manipulate the process of intrusion and detection for a standard arbitrary system.

Prevention Mechanism of Cyber Security Incident .

It includes the standard operation procedure of setting up cyber security information system, offering the cyber security technology and management advisory service, doing the network patrol, the simulation of a cyber security incident and the emergency drill, holding relevant education and training participating in international computer forensic exchange of technology and international cooperation, training up the computer forensic specialized personnel, construction of the honeypot system, setting up the characteristic database of national network, etc. As computer crimes are growing rapidly, computer forensics is becoming more impartment.

The law enforcement agencies around the world take cyber forensic as an imminent challenge. High technology crime would be much more harmful to the society as a whole than traditional crime. Furthermore, all sorts of crime, like sedition, treason, corruption and bribery, economic crime, drug trafficking, and money laundry, and so on, would utilize high-tech devices and network as tools of criminal acts. Besides FBI, cyber forensic has higher priority in the law enforcement agencies than computer crime in the U.S. China should accelerate work in the cyber forensic field to cope with the high-tech crime era.

There are initiatives to setup new laws and legislations to combat cybercrime by relying on a proactive collaboration of involved parties. For example, the Dutch ministry of economic affairs has recently proposed a new law that concerns those parties that collect personal information and, due to some reason, lose their control on this information. Such parties are obliged to report on such information leakage incidents as well as on their countermeasures to the Dutch Data Protection Authority (CBP, het College Bescherming Persoonsgegevens, in Dutch) and to those individuals who have lost their personal information. The objective of the proposal is to increase the riskawareness of such parties who store sensitive information in high volumes; to encourage them to investigate better the reasons behind data leakages, and to stimulate them to adopt better measures to protect private data. Moreover, when informed on time, individuals can personally take immediate actions to rectify their information breaches such as blocking their bank accounts. As another example, a new European data protection law is being proposed these days that mandates issues like the right to be

forgotten. When this proposal becomes legislation, individuals can gain control of and exercise their privacy rights more directly than it is possible nowadays.

Government Response and Recommendations .

To effectively address these challenges, the regulator must possess knowledge, strong links with the industry, avenues for international cooperation and authority to enforce law. The availability of resources, skills and technology so as to identify vulnerabilities, assist service providers and users, predict and detect criminal activities are also necessary for a sound e-banking regime. Moreover, China ought to establish jurisdiction agreements with other states in order to deal with complex cross border electronic financial transactions and activities.

While the government and the law enforcement agencies should lead such initiatives they must also liaison with intermediaries and the industry with a view of not only addressing their concerns but also providing the means to deal with challenges.

We wish to collaborate with the countries around the world, For example, we have already reached common consensus of international criminal law cooperation with the U.S to combat high-tech crime. (1)Work support and strengthen the crime investigation squad: Trough Work support of with special forensic department and investigation of computer crime to strengthen the effect of combat crime our country. (2)Computer and network security assessment through out the organization, and assist other government unit to evaluate their security measure. (3)Communicate with academic institutions, and collaborate with government units, IT corporations, and professionals to advance the development of cyber forensic technology. (4)Be participating international symposiums and organizations to promote international cooperation, and to associate with other nations to support with each other.

Conclusions

The virtual world has also provided a hugely spiraling and apparently uncontrollable platform for crime and illegal activity to thrive and prosper. It is clear that to combat cybercrime, cyber security, cyber terrorism, and cyber warfare effectively does require an interdisciplinary knowledge and international collaborations. The law of a nation could not sufficiently govern multi-jurisdictional crime without violating the sovereignty of a nation; the best approach to solving universal crime is by creating universal law. Eligible for punishment can be included in China's penal system, as new types of penalties. Eligible for punishment including the public authority, parental authority and occupational deprivation of the right. Computer and cyber crime as a high-tech career criminal, set or provide deprived of their professional qualification in computer and networking industry, will play a very prominent role in the containment and prevention of crime.

Acknowledgement

The work presented was supported by Henan province government decision-making research project bidding(No:2013B104).

References

[1] W. Chung, H. Chen, W. Chang and S. Chou, "Fighting cybercrime: a review and the Taiwan experience," Decision Support Systems, 2006,vol. 41, pp. 669-682.

[2] Han Zhe. The essential characteristics of cyber crime and its criminal jurisdiction [J]. Shandong Public Security College, 2002 (3): 68-71.

[3] Lu Yao. The meaning of computer and cybercrime legal perspective Study [J]. Beijing University of Posts and Telecommunications (Social Science Edition), 2010 (2): 24-28.

[4] Cyber crime cases continued to increase attention should be paid [EB / OL], http://news.xinhuanet.com/legal/2010-09/12/c_12542964.htm.

[5] The concept of computer crime in the Penal Code [EB / OL], http://www.lawtime.cn/info/xingfa/jisuanjifanzui/2010110275983.html.

[6] Li Jin yuan, Analysis of computer crime challenge the existing criminal law and criminal legislation to improve, http://fjfy.chinacourt.org/public/detail.php?id=10280.

[7] Neil Barrett. "Digital crime" [M]. Hao marine Translation: Liaoning Education Press, 1998,2(6): 1876.

[8] UK seeks next generation of cyber security specialists, Retrieved from, http://www.bbc.co.uk/news/uk-politics-11715177 as of February 9th, 2011, (2010).

[9] UK decides to opt in to EU-wide cyber security plan, Retrieved from, http://www.bbc.co.uk/news/uk-politics-12354931 as of February, 9th, 2011, (2011).

[10] H. W. K. Kaspersena. Computer-related crime, information security and investigation of crime: A delicate triangle, journal International Review of Law. Vol. 9(1), pp.129 – 141:Computers & Technology.