Internet and computer crimes

[1]Ramin Delkhoun Asl, [2]Saeed Delkhoun Asl

1. Faculty of Human Sciences, Payam-e Noor University of Ardabil, Ardabil, Iran
2. Faculty of Human Sciences, Ardabil Town Hall and Village assistance university of Applied and Technology, Ardabil, Iran

Abstract: The computer crimes are those crimes originating from the modern technological issues and considered as artificial events having their own features. The features such as fast and easy commit crime, the lack of physical appearance in committing a crime, hyper-territory and motivation of a crime and achieving it in an intangible setting are being considered its real features of the modern technology in this regard. Hence, computers are suitable cases for committing crimes as well; in the other hand, with development of computer technology, fighting challenges have been complicated against them; in the field of international law and regulation affairs also these have been newly called for urgently; substituting the law issues have made judiciary officials with too much problems; along with computer, the internet and the third generation (cyber space) have been added to these problems making many problematic issues in this consideration.
[Ramin Delkhoun Asl, Saeed Delkhoun Asl. **Internet and computer crimes.** *Life Sci J* 2013;10(2s):139-143] (ISSN: 1097-8135). http://www.lifesciencesite.com. 23

Key words: computer system, communication system, information system, service provider

1. Introduction:

In every society various people are often waiting for opportunities to make their abuse application in every time; these opportunities may come from other people neglect and being a great chance for abusers; with the development of technology and available information issues at people's hand, criminals have been increasing, too. In this internet space, there is no any geographical, distance, time and national restrictions; in a new situation, the computer crimes have been increased incredibly. By the progression of the technology, the numbers of crimes are being increased; these crimes are also changing into international crimes, too. As you know, the most sensitive actions such as banking issues, trading shares, selling & buying and managing personal accounts are being achieved by computer and internet. Although computer is making an easy way for the whole transactions and personal affairs but it can make a great opportunity for hackers to break their setting out; these new threats like spy soft wares and internet cheating have been appeared. These threats are being achieved by some cheaters on the net financially along with more complex achievements. These are the new challenges for those ones working on the internet dreadfully.

Research methodology, obstacles and problems:

Due to the new appearance of the topic, the author had also some problems in the field of using books and various references in this regard; as you know, having accessibility to foreign resources with new topics is not easy; to write the related article, the quality-based method (library researches) and internet were used efficiently.

Hypotheses and research questions:

By studying and seeking the computer and internet facilities, I got familiar with new terms of the related issues. These issues require an independent way; issues such as legislation at internet issues and the responsibility of internet service providers, how-to-know committing crimes, the role of internet industry and fighting against hackers, training children by peers and parents and making centers for reporting the sacrificed people in this regard. The main hypothesis here is mostly subjected to the features of these crimes; these crime have their own specifications being done easily; the other hypothesis is that issuing a legislative and criminal policy are required for confronting against these crimes and computer recognition, internet and cyber space as well as facilities and threatening settings. The main purpose of the study is to represent the needs and necessities and giving approaches for responding the needs in this regard. These questions may be as following:

How do these computer and internet crime achieve? Who are these criminals' features? Who are the most susceptible people to these crimes? How are the degrees of these crimes on sacrificed ones? What does a society do against these? What international approaches have been fulfilled against them?

The history of changes?

The growth and development of new and modern life has been vastly changed these days; the history of these kinds of crime dating back to the changes of information technology in 1960s when the first case is called computer crime. These have been reflected into those times magazines including the first

and simple spying computers and destroying or abusing illegal applications of computers. Generally, the history of the computers can be categorized into three generations; the first generation is devoted to the late of 1980s by the title of computer crimes including robbing and coping programs at computers in private territory; by the development of technology the second generation of computer crimes appeared in 19990s calling crime against data including stealing and attacking against the whole information technology, communicative and computers and satellites as well as international webs; in the middle of 19990s, the third generation of computer crimes have been emerged by the name of cyber crime being constructed in cyber space including the whole international and regulations related to computer setting as well; in the middle of 2000 coincident with the fast growth of computer technology, these crimes become the new form functionally; in this decades, in addition to specifying the crimes, other new crimes such as smuggling the words on the net, committing at cyber space(virtual setting) or other multi-media crimes start appearing in this case.

First chapter: internet and computer crimes- first discussion: definition of computer and internet crimes:

a- Computer crimes: there have been given many definitions in relation to computer crimes but no any formal description made in this case yet. Because there are many different comments making the foundations of computer crimes; given definitions have their own applications; for the first time, O.E.C.D has defined the computer crimes in 1983 in relation to computer misuse at that time. According to that organization: any misuse of computers including any illegal behavior and unauthorized regulations against computers related to data is not authorized. In different countries, there are various comments about this pointing to some of them here as following:

According to the definition of Germany criminal police federation, computer crime is including the whole situation and issues where the electronic processing of data has been considered as a tool for committing crimes at computer setting. According to an Austrian professor, the computer crimes are including criminals being achieved at computer setting. By the supervision of the US superior court, any wrong function against computers at web-based setting should be prosecuted as a computer crime.

b- Internet crimes:

The internet is the world of the computers; this includes numbers of websites being connected together for sending any messages or e-mails by the way; the sent information has not got a pre-defined path and the internet is the best place for the related path even if those have been sent from other countries; based on a given theory, if someone lives 100 year old he or she can get just 3 percent of the internet; the source of the net dates back to 1970 and computer webs conference(local-internal). At first, it was named Arpanet; during the time, there have been many changes in this regard constructing the structure of the internet globally. The internet cannot be considered as a computer net or a collection of computer webs connected together. In fact, internet should be observed as a gigantic source of information letting millions people to connect together in the world. Thus, you can easily interact and connect or send your messages together in the world. So, the internet crimes are the complementary issues of computer crimes particularly the third generation of the crimes as cyber crime.

Second discussion- features of computer and internet crimes:

The internet and computer crime are distinct crimes together which not only makes the regulations hard, but also they make problems at the field of law.

Computer crime committers:

The computers committers are belonged to rich and open-minded people; generally, the age of these criminals ranging from 10-60 year old. The most dangerous crimes and financial wrecking can be considered from the hackers with college history.

The lack of the subject at criminal scene:

In most crimes the existence of the subject is necessary for achieving the criminals but the subject does not exist during committing crimes.

The lack of time and place restrictions:

The computer crimes have little restrictions; for example for stealing a bank time or needed for the steal to achieve it efficiently but the computer crime is possible in a short period of the time. For example the top secret information of a military base can be taken place at a few seconds. The place restriction does not exist in computer setting, too. The computers connecting to other centers just through a telephone line can be stolen easily. Not only stealing but also other crimes can be done by this way.

The hyper-national and international features of internet and computer crimes:

One of the most essential features of computer crimes is subjected to their territory internationally causing to destroy the vast territories. Due to the nature of computer crimes no any restrictions can be found in this regard.

These can be happened without the appearance of the subject.

The method of collecting reasons and prosecution at computer crimes:

In computer crimes there cannot be found any documents; it is subjected to their main and first features of the computers; that is, removing the extra tools and giving the fast media in achieving the affairs which it makes the process complex. For example in cheating any writings cannot be prosecuted; the type of research, evaluation the crime scene, stopping the tools and other skillful experiences cannot lead to the discovery of crimes.

Second chapter- how to prosecute the crime and fighting approaches and prevention of internet and computer crimes:

First discussion- how to follow the computer and internet crimes:

With the development of the technology and appearance of the crimes, the law has been gotten into some problematic issues; in this technology, the reasons are being intangible and invisible; and this made problems in the follow-up the crimes and their record in this regard. At present, one of the biggest problems of the countries is referred to the prevention methods about computer crimes. As mentioned before, these crimes have their own features leading to the arrest of the criminals. In this discussion, the law problems and prosecution issues by the title of the basic introductory data evaluation is being reviewed.

First part: introductory researches:

The first problems in this case are due to the existence of material based computer crimes through the entrance and changes of data being achieved by communication centers. In computer crime we are challenging with digital setting and they affect on the same criminal functions; the criminal rights has been paid attention towards the tangible material targets; hence, the laws have been carried out for the reason; now the question is that what is researchable in the digital environment? Are the officials able to seek the related crimes and try to prevent them? In fact, given information are the new form of the computer data which have been kept at the time of prosecution court; the basic researchers are the most essential part of the criminal court in relation to discover the crimes. For the reason, these officials should have enough skills and experiences to collect data in this regard; in most countries, there are special expert groups for discovering the crimes efficiently.

Second part: evaluation and recording data:

Assessing and prosecuting data are the most effective tool in computer crimes; collecting data is subjected to computer systems; now, according to prevention regulations, the data are considered as the tangible things or no? In addition, this problem stated that recording data may hit other activities or personal rights as well; to discover the data and aware of the crimes, the correct completions of the law affairs are needed as following: hiding the criminals, the effects of invisible data, coding the data and documents, destroying the data and information, majority of data and inexperience of law officials.

Second discussion: fighting approaches and prevention of computer and internet crimes:

At present, living without computer and internet is not possible; in recent years, this technology has been increasingly inaugurating; for example, there are many different entertainments in the field of computer to trading issues; in fact the men are relied on the computer life; unfortunately, the steals and cheaters abuse other people which made working on the net complex. These criminals are increasing these days. They mostly like to destroy and enter others privacy to copy their files and even their moneys, too. In the criminal rights like other fields there are new based forms of laws which one of them is subjected to computer crimes. These laws try to find and determine the criminal actions approaching to new preventive ways as well; in the other hand the criminal sciences try to find best solutions for preventing the computer and internet-based crimes; these issues are most discussable.

First part: preventive approaches of computer crimes:

The task of the governments and officials are related to apply methods of prevention in this regard; the experiences of the most countries in this case representing their strives in the field of preventive actions so far as following:

They have tried to make an interaction between the community and executives of the law.

Not only the three organization of legislation, judiciary and police but also other organizations are responsible for achieving their bests at this filed.

The necessity of changing at regulations:

According to the fast growth of the computer criminal actions, there have been achieved some promising steps towards the users; the struggles of the legislative affairs in fighting against the crimes should be changed; for example, the internet does not possess to any geographically territories; no any post or position exists here. The pioneers of these approaches can be pointed to the US, Canada, Germany and Greece; in addition, in the

US and the Netherland, there have been strict legislations against any computer crimes.

The role of internet service providers (ISP) in prevention of computer crimes:

Many computer crimes can be achieved at World Wide Web (WWW); hence, it is necessary for the providers to consider what they fulfill on the webs. Usually, in the study a crime happened, two categories play key role as following:

Information related to customers accounts

Information related to each session connection through the net;

For the reason, internet providers play key role in prevention of computer crimes.

The legislative executive officials cannot achieve anything without the cooperation of the community; some approaches done in this field are as following:

There is a fundamental foundation that every person or organization is responsible for caring the data itself.

The boost of anti-virus software and its distribution with suitable price in the society. Also designing antivirus software particularly for the preservation against any attacks.

The organization along with their achievements in relation to their spiritual territory rights should apply care software not to be easily transferrable to others.

The role of government in prevention of internet crimes:

In contrast, the governments should publish the interaction culture of conversation in the community. This can be done along with the following approaches:

Representing the data privacy establishment in the strategy of government and private section.

In the legislative terms, the cooperation of private section should be carried out efficiently. The legislative officials should make their prevention against criminals; these information necessarily should be devoted to providers of data and industrial sections as well; the government should continuously evaluates the criminals timely; the publishing of moral culture in information space; applying safety and preventive approaches to reduce the computer crimes.

Second part: how to technically confront computer crimes:

The experience showed that the unsuitable safety system facilitates computer crimes. Therefore, fighting against computer crimes has its own importance as following:

Using antivirus software:

These can be appeared against those unknown viruses and protect computer.

Using anti-spy software:

The best way for protecting computers against spy software and Trava horse; both these soft ware's can prevent other viruses as well and stop installing destructive software.

Using Firewalls:

It is a kind of software or hardware that handles the computer connection to other communicative tools; then, it checks the whole entrance of software and secondly, it supervises the transformation data to computers.

Filtering porno programs:

As you know, the inventions are the basic requirements and this can be true in relation to pornography issue. In the years where researchers fight against the porno, the best approach is subjected to filtering these programs. The result is that there is a complete tool appeared in the market fighting against the pornography.

Coding files and profiles:

If you have so sensitive files such as accounts, coding desktop is the best option particularly if computers are stolen; the coding is best choice for protecting them in this regard.

Filtering search engine:

Putting filter on the search engines such as Google and yahoo,… can be a great way for protecting computers from hackers; it of course does not need any software assistance.

2. Conclusion:

The growth and development of new technology in our life has been considerably changed; today, using computers at various locations have been devoted to many actions as well; the same growth has been made many different problems for users. The problems are related to discovery crime, certification, how to evaluate, how to prevent and the lack of cohesion with criminal courts and legislations. The internet is the huge connection of the computers in cyber space and considered as a key global element in the world. In a place where the whole technological affairs can be fulfilled easily, the new horizons waiting to be opened in the world. It is interesting that the most fruitful tool for the new generation of the man is getting to become or bring the worst consequences now; the pornography and children abuse are those cases that can be done through the internet, too.

As mentioned before, these computer crimes are related to those cases that having the national and international nature. So, these have completely international nature should be prevented as well as making new approaches in this case. In most countries filtering is the greatest method for preventing pornography issues; however, the

gigantic space in the net is making the terrible problems to use censorship easily, unfortunately. In fact these countries try to make their challenges against the pornography and other criminals. Any legislative control should be supported by people and institutions as well; we should focus on the net because the era of the newspapers has been disappeared; if the judiciary official closes a website, other one start opening along with new address; unfortunately, no way exists to follow these websites easily; hence the ability of order ship is complex here.

Recommendations:

In order to handle the computer crimes globally, it is necessary to submit regulations between countries. The public participation and cooperation should be achieved particularly by private and government sections. Installing information sensitive centers to protect the systems. These centers are being supported by the Electricity College, computer and scientific supportive rights and defensive ministry. The governments should make a great background for executing their regulations as well and to be confident of their reports between other governmental policy makers departments. The boost of antivirus software in a community particularly in privacy centers. Training related personnel in completion of the legislations. Making fighter groups against any computer events such as FIRST which started in 1990 with 11 members and now it is working with 50 members actively in North America and Europe. In the Asia district APCERT is a team working actively as a safety group in China, India, Malaysia and Japan. Optimizing the scientific level of colleges about the legislation and computer through 2 unit lesson at college. It should be noted that the law colleges should also be pioneer in this regard but unfortunately no any steps moved in this issue.

1/8/2013

References:

1. Bastani, Broumand. The computer crimes and internet, (new appearance of criminals), Behnami publication, 1st printing, 2004.
2. Bouje, Gayvander. The comments for prevention of computer crimes; Translated by Mohammadhassan Deghiani; the informatics council; the organization of the budget and planning, 2nd volume, 1997.
3. Khodagholi, Zahra; computer crimes; Arian publication, 1st printing, 2004.
4. Ziber, Olrisch; internet crimes, Translated by Mohammadali Nouri and Reza Nakhjavani and Mostafa Bakhtiarvand and Ahmad Rahimi Moghadam; Ghanj Danesh publication, 1st publication, 2004.
5. Farzane, Fateme. Privacy at internet; Naghous publication, 1st printing, 2005.
6. Internet websites:
7. www.iritn
8. www.systemgroup.net