The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 2 || Pages || PP -23-27 || 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Effects of Cybercrime and Ways to Deal with it

Mohammad Ali Bani Younes
Department of Computer Science, Ajloun National University

ABSTRACT

With the continuous growth in the information theory (IT) revolution, we are facing many sudden dangers and problems that accompany any civil and technical development. Technological advances that carried advances to all aspects of life including crime methods and tools have led to the emergence of what is known as electronic crimes. A development in the size of the electronic crime and the way it's used has been taking place. This caused new crimes that were not known before to arise as a result to what has been achieved in scientific advances and technical development and whatever accompanied that as social and cultural changes on all societies. This research has addressed the ways to keep up with modern technology and how to secure it once it is spread, how to put it to work in the field of crime prevention and control and how to provide qualified and trained manpower to work on these new equipment to achieve high performance. It also discussed the means of cyber crimes and prevention methods in order to make people aware of it and its damages.

Keywords - *Cyber crimes, cybercrime definition, types of cyber crime, cyber crime goals, prevention methods of cyber crime, Perpetrators, means of cyber crimes.*

Date of Submission: 02 January 2016 Date of Accepted: 19 February 2016

I. INTRODUCTION

With the development of science and the spread of IT technologies in our time, which is witnessing a massive information revolution, where different sciences and discoveries race to emerge in every day announcing a strong and sharp competition in this area. In the beginning, the World Wide Web (the Internet) emerged with its limited usages, however, it has expanded and spread rapidly in a record time, with users of all age groups and at different levels of education; and thus opened the closed doors and rang the alarm as this network remained unguarded and without restrictions or limits to deter bad deeds originating always from human beings. For this reason, and as an inevitable result of any technical progress novelty led to the emergence of so-called cyber crimes that came to alert communities of its great danger, as it expanded its scope and its professionals had emerged stealing, looting and causing destruction. This led communities to acknowledge the necessity to take a tough stand towards them and to find solutions quickly. The core of these solutions was to find the essence of cyber crime, its purpose and forms and how to stay away from it and those who belong to it. This is true because the first step in a treatment is to know the disease. This caused the emergence of the importance of knowing cyber crimes and the necessity to educate people about its danger and objectives[6,8,9].

II. RESEARCH SIGNIFICANCE

The importance of this search is to know the essence of cybercrime, their purpose, and to know their forms, and how to prevent the society from the cybercrime and its owners. The first step~~s~~ of treatment is to determine the disease. So, the importance of knowing cybercrimes and its forms has come out as well as the necessity to educate the public about its danger and goals and what harm it causes to society. It also encourages the concerned authorities to enact lows that deter such crimes. This research provides a comprehensive definition, and description of cybercrimes and to know the perpetrators of these operations. It also provides a comprehensive definition of the types, brands, means, and some details about the committed crimes, as well as the prevention methods of it in practical life~~.~~, which helps to increase awareness of how to reduce them.

III. RESEARCH PROBLEM

The research problem focused on cybercrimes and its danger, which prosper with the collapse of community values. Technological change, which has been witnessed all over the world, the large development in communications that came out of this change and the many new technologies have a big impact in the appearance of one kind of crimes that differs greatly in its look, methods and perpetrators from the meaning of crimes in its conventional forms. This new type of crimes is called cybercrimes. Its danger is increasing daily especially with the increase of internet users. Negative scientific and technical side effects of this type of crimes was eluded to by a study which indicated that they increase the gap between developed and developing countries, as these countries have become a monopoly of information, hijacking computer centers, as they are stealing information by several methods, including breaking down this information, change or reproduction of data, or send viruses or disable computers. This makes it as a that is equivalent to the power of a conventional war being waged by some countries, which is fighting using its real weapons. The only difference is that the weapons here is a computer and informatics to paralyze the other party and to influence him psychologically and politically, scientifically and technologically [4]. This in addition to the negative effects and the many related aspects and moral values to them.

IV. RESEARCH OBJECTIVES

This research attempts to discuss the following topics in details:

- Definition of cyber crime.
- Goals of cyber crime.
- Perpetrators of cyber crimes.
- Types of electronic crimes.
- Forms of electronic crimes.
- Characteristics and attributes of electronic crime.
- Tools of cyber crime.
- Prevention ways of cyber crime.

V. DEFINITION OF CYBER CRIME

Cyber Grime can be defined as a set of illegal acts that conducted through tools, electronic devices, or the Internet. Thus, this type of crime requires the specific knowledge in computer techniques, its systems, and the various of the computer program, so that, they can commit such crimes. It can also be defined as any illegal act in which the computer is used as a tool or the subject of the crime, where the criminal can get different benefits, causing harm and loss to the victim. In addition to the above, cyber crime can be defined as any violation committed against individuals or groups, intent to abuse the reputation of the victim or his body or his mental manner directly or indirectly, through modern means of communication [1,2].

VI. GOALS CYBER CRIME

The goals of this research are:

1. Penetrate servers that are serving information and then disable them.
2. Being able to access information illegally such as stealing information viewing, deleting, or modifying it, in order to achieve the goal of the offender.
3. Blackmail those who use technology, such as institutions, banks, individuals, and government places, by getting their own confidential information
4. Achieve gain illegal materialistic gain, such as credit card fraud and theft of bank accounts. In addition, achieve the political and moral gain through destroying or distortion of internet sites.

VII. PERPETRATORS OF CYBER CRIME

Perpetrators of cyber crime can be classified into two categories[4]:

1. Specialists, professionals and terrorists who deliberately cause damage to others. This harm could damage big corporations as well large countries.
2. Children and adolescents who do not realize the extent of the damage that they do, because their motives are mostly just for fun and to prove they have a supernatural ability with respect to others.

VIII. TYPES OF CYBER CRIME

The main types of cybercrime are:

1. Crimes related to secrecy and safety, which includes [2,12]:

- Illegal entry.
- Illegal objection, which is the Interception using technical means for the transfer of input or output
- data from/ to computer network or during the treatment process in the computer system.

- The destruction of the data, change it, disable it, or distort it in order to the make it unusable.

2. Crimes related to counterfeit and fraud, which is aimed at software piracy such as infringement on the rights of authors.
3. Crimes related to persons and money, this selects the people, where it is possible to kill them by using the computer as a tool. Or selects the personal property to destroy it without being stolen.
4. Crimes related to a personal property, this targeting electronic information, that is stored on devices, do that modify, or change the information stored on the devices, or pick up messages sent between devices for distorted.

IX. FORMS OF CYBER CRIME

The main forms of cyber-dependent crime are outlined below[5]:

1. Websites' cybercrimes: This is represented by the illegal entry to the systems and to the data processing rules, regardless if data manipulation took place or not. Just the illegal entry to websites is considered a cyber-crime. It is also represented by the attack on the websites, whether it took the form of deleting, modifying, manipulating the data, or blocking the operation of the system.
2. Cyber-Crimes of Personal Data: There are some limitations regarding the establishment of computer systems. Dealing with information, which leads to breach in confidentiality and privacy is prohibited. Using data for purposes different than what it was collected is also sprohibited.
3. Crimes of Attack on The Electronic Funds: Electronic funds are traded electronically, whether in the context of e-commerce, or others such as withdrawals and deposits at the ATM machine. These funds, similar to regular money, can be the object of theft, fraud, and breach of trust, as the payment of e-commerce depends on the electronic fund transfer, or the use of electronic credit cards, and the use of digital money. One form of cybercrimes funds is the use of expired credit cards or canceled cards by the authority that issued the cards or the use of stolen or forged credit cards. Another form of cybercrime funds is the infringement of third party funds by electronic means such as access to sites of the banks, access the customer accounts, whether by entering or deleting the data for the purpose of misappropriation of funds or transported and destroyed.
4. Signature's Cyber Crimes: Electronic signature is a set of electronic codes. These codes are capable for distinguishing the signature of the owner from another. The electronic signature considered as a tool or a way for the adoption of electronic transactions, it serves as a written signature on paperwork, so it means that any action considered against the law, if that action intended to fraud the electronic signature, or use it without the knowledge and consent of its owner.
5. Consumer's Cyber Crimes: In general, laws provide consumer protection. The electronic consumer is also entitled to these protections, Acts such as the misuse of customer's information or taking advantage of customer's unawareness to commit terms he/she does not know are considered cyber.

Other Crimes: There are other crimes that are committed by intermediaries who provide Internet services, such as transport services, connecting a client to the network, or information storage, production or supply. In addition, tax evasion crimes in e-commerce is also considered part of cyber crimes. E-commerce, is similar to regular trade, it is subject to the same laws and procedures of customs and taxes, fees, and other financial obligations, therefore, any breach of these procedures in the framework of e-commerce is classified as cyber-crime

X. CHARACTERISTICS AND ATTRIBUTES OF CYBER-CRIME

The main characteristics and attributes of cyber-crime are outlined below [3,6]:

1. Ease of committing the crime away from the security control.
2. Lack of clarity of the size of the damage caused by cybercrime.
3. Difficulty to identify the offender or determine the identity or location.
4. Deficiencies in the laws that punish criminals who commit such crimes.
5. Geographical distance between the offender and the victim.
6. The speed and anonymity of cyber attacks.
7. Evidence against criminals can be get rid of easily.

XI. EXAMPLES OF CYBER CRIME

Famous accident is what happened three years ago to the internet site of the Central Bank of Egypt, where the attacker logged in illegally to the server machine that is being broadcast from, exploiting one of the vulnerabilities and he changed the main page of the site, which caused confusion among its customers fearing that the attack may have extended to other banking transactions. Another incident involved group that made a site on the Internet under the title of (http://www.gatt.org). This site was showing the fifth result in most search engines for the WTO. It has been used to get the email data and the rest of internet users data who were originally trying to visit the World Trade Organization. The case with the World Intellectual Property Organization is still pending. On April 7, 1999 one of the financial news magazine visitors which was Managed by Yahoo Foundation sent an email message under the title of "Sale News". The message included that the PAIRGAIN company was purchased by an Israeli company, also the letter contained the link to one of the sites that offer new services offered more details on this news. As soon as the news spread, the company's shares have risen 30 cents, and trading operations grew and increased about 7 times, but there was a problem, which is that, this news was not true the site that was included the details was also an imaginary site. When news spread that the above information is incorrect the stock prices fell horribly. Therefore, this event caused huge financial losses to many investors who bought those shares based on the first news. After a week of the incident the FBI arrested a man from North of Carolina. This person was considered one offender, and he will not be the last who used fraud websites. He was prosecuted through the Internet IP address, He was accused of fraud by publishing false information about the shares of joint stock companies, A civil suit was held against him for compensation for damages caused to the investors. Finally, in August 1999 he was sentenced to five years in prison and to pay the amount of $93,000 [1,7].

XII. ELECTRONIC MEANS OF CYBER CRIME

The types of Electronic Means of Cyber-Crimes are outlined below[8]:

1. Antivirus or anti-virus software are one of the most widespread and common crimes on the Internet
2. Trojan horse is a small code loaded with very popular programs, that do some hidden tasks, often focused on the weakening of the forces of the defense of the victim or his computer penetration and theft of data.
3. Identity theft.
4. Turn off the services of servers by dumping a huge number of requests, leading to an imbalance in the server and its immediate shutdown.
5. Defamation by publishing information obtained by the offender illegally.
6. Fraud such as the sale of goods or services phantom.

XIII. PREVENTION METHODS OF CYBER CRIME

The prevention techniques of Cyber Crime [10,11]:

1. The development of the family and community role to face cyber crime through educational flyers, hold awareness conferences and distribute guideline papers on Internet pages.
2. Take caution and not to believe all of the advertisements and make sure of its credibility through the famous search engines and avoid opening any anonymous email and hasten to delete anonymous messages.
3. Design a lot of software that work as a firewall against pirate attacks.
4. Develop laws to curb from cyber crime of the world with the international organizations help.
5. It is important to ensure validity of electronic titles that require confidential information such as credit card and bank accounts.
6. Passwords should not be disclosed to anyone and to ensure that it is updated periodically and selecting the mystery of unfamiliar words.
7. Do not download any file or program from unknown sources.
8. Not to publish photographs online.
9. Keep backup copies of files and folders for reference in case the originals get lost or exposed to viruses.

XIV. CONCLUSION

As technology shortens the distances between people by providing many communication and transportation means that were not known before, it produced many negatives. One of the most important ones was the difficulty to maintain one's privacy due to the spread of tools that are easy to use by the World Wide Web pirates. Cyber-crimes are new and they are not covered by the traditional criminal law, thus there is no texts of the Penal Code that relate to electronic crime, therefore, it is difficult to make judgments against perpetrators. The judicial organs and law professors are still unable to come out with a clear vision on cybercrime. The law does not punish for stealing information as it is considered immaterial. The main problem is not the exploitation of Internet criminals, but in the inability of the justice branches to prosecute them, and to keep pace with new technology. There is a major development occurred in the magnitude and methods used in cyber- crime. There are also modern crimes that were not known before. However, modern electronic technology has played a role in both of them (magnitude and methods), and what happened as a result of scientific progress and technical development, and the accompanying social and cultural changes not at all communities. So, modern technology used immediately after deployment and put them to work in the field of crime (prevention and control), and to provide qualified and trained manpower to work on these modern devices, to achieve high performance through the use of scientific research in the monitoring and counting and exploring movement of the crime, in order to keep up with these crimes and reduce the aggravation.

XV. RECOMMENDATIONS

This research yielded the following major recommendations:

1. Educate family and children about the risks posed by cyber- crimes.
2. Fill the legislative vacuum of the fight against cyber-crime, and to include the substantive and procedural rules.
3. Granting authorities the right to seize, investigate, and conduct an inspection and control of any particular crime technique that help to prove it.
4. Preparation of systematic judicial system to deal with cyber crimes.
5. Create a national committee of various institutions and community sectors to counter the danger of cyber crimes.
6. Hold international agreements to counter cyber crimes and to hold accountable those who do.
7. Create a proactive treatment ways to prevent the occurrence of cyber crimes.
8. Invite the media to investigate in its news and sources before the publishing process, and to look at the role of the administrator in the public awareness and alert him to the dangers of abuse and the use of modern technology.
9. Understanding the use of modern techniques to avoid victims of the cyber crime.
10. Enabling infrastructure that rely on technology and information systems and to prevent the occurrence of any electronic penetration through the group work of all the institutional, legislative and academic efforts, to face the different types of cyber crime.

REFERENCES

[1] Prof. Dr. Marco Gercke, *Understanding cybercrime: Phenomena, challenges and legal response* (e ITU publication, September 2012).

[2] Dr. Ajeet Singh Poonia, Cyber Crime: Challenges and its classification, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* 3(6), November-December 2014. Web Site: www.ijettcs.org.

[3] H. Saini, Y. Shankar Rao, and T.C.Panda, Cyber-Crimes and their impacts: A Review, *International Journal of Engineering Research and Applications (IJERA), 2(2*), Mar-Apr 2012, 202-209.

[4] S. Malby, R. Mace, A. Holterhof, C.Brown, S. Kascherus, and E.Ignatuschtschenko (UNODC), *Comprehensive study on cybercrime* (United Nations New York, Printed in Austria, February 2013).

[5] Dr. M. McGuire, S. Dowling, *Cyber crime: A review of the evidence Chapter 1: Cyber-dependent crimes*, (Home Office Research Report 75 October 2013) 4.

[6] N. Khadam, Insight to Cybercrime, *LAW FORUM 29(1), Federal Bureau of Investigation's* 2010 statistics.

[7] N. Aseef, P. Davis, M. Mittal, K. Sedky, A. Tolba, *Cyber-criminal activity and analysis* (White Paper Fall 2005).

[8] J. Ashcroft, *Electronic crime scene investigation: a guide for first responders* (Written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, July right, 2001).

[9] R. Smith, Book review of cybercrime and society, *Australian Institute of Criminology, Australia, International Journal of Cyber Criminology, 2(2)*, December 2008, 397-399.

[10] Ms M Lakshmi Prasanthi , Tata. A S K Ishwarya , Cyber crime: prevention & detection, International Journal of Advanced Research in Computer and Communication Engineering, 4(3), March 2015.

[11] M. Fra , Cybercrime prevention and awareness, *To join conference call dial (305) 433-6663 option 4 PIN # 42014* , April, 2014.

[12] Ms. M. N. Muley, cyber security in the era of networking: A Review, *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18(1), Ver. III,* (Jan – Feb. 2016), 18-21, www.iosrjournals.org.

Mohammad Ali Bani Younes, was born in 1962 in Irbid where he grew up and had his education. He got a Bachelor degree from Yarmouk University from the Computer Science Dept. in 1986, masters degree in Computer Science from Sudan University of Science and Technology in 2003, and the PhD in Computer Science from University Science Malaysia, Penang in 2009.

He worked as Assistant Professor in the Computer Science Dept at Irbid National University from 2010 until 2013 .Currently, Dr. Bani Younes works as an Assistant Professor at Ajloun National University at the Department of Computer Science, Jordan. He is interested in teaching computer science.