J. Basic. Appl. Sci. Res., 3(3)952-957, 2013
© 2013, TextRoad Publication
ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Organized Cyber-Crimes, An Approach on Islamic and Iranian Legal Systems

Mahmoud Malmir, Ph.D.

Assistant Professor of Islamic Azad University, Khorasgan Branch, Isfahan, Iran

ABSTRACT

An organized cyber-crime is a new issue which is gaining arising significance among the lawyers and legislatures. This sort of crime has unstable situations; so some of the jurists have major doubts about their existence. But as we will discuss, this opinion is not acceptable and we believe cyber-crime is a fact. Organized cyber-crimes whether official or not official, are an expanded problem. Different legal systems provide various sanctions against these crimes, but Iranian penal law does not have a specific code for this reason, although some roles may be derived from Computer Crimes Code.
This research is based on accepting cyber-crimes and cyber-terrorism. We will try to determine the cyber-crime and its boundaries, to reach an opportunity of systematic prevention of such crimes.
KEYWORDS: Cyberspace, organized crimes, criminal cyber micro cultures, Iranian legal system.

1- INTRODUCTION

An organized cyber-crime seems to be a combination of cyber-crime and organized crime; but precisely it is an independent issue which has its very own essence. To study such crimes, one should know the followings: cyberspace, cyber-crime and organized crime. We will define these concepts at first.

1-1- Cyberspace:

The term "cyberspace" first established in 1982 by William F. Gibson, the Canadian author in his science-fiction story "Burning Chrome" and popularized in 1984 by his book "Neuromancer". In 1990 professor John P. Barlow used this term in an online conference and made it common afterwards [1]. "Era of information" or "Era of computers and networks" draw a globe based on computer networks on which even the traditional human relations are transferring into a cyberspace. At first we should define the terms "space" and "cyber".

Space is a concept of "where", even though place is concept of "somewhere". Place has a containing but space does not. Place has two dimensions but space has three. Place has borders but space is infinite [2].

Cyber is derived from Greek word "Kybernetes" which means pilot or navigator. The term Cybernetics first used by mathematician Norbert Wiener in his book in 1948 [3]. Cybernetics is a science to study and control mechanisms in human, animated and computer systems. In this science the classification of information is emphasized. The term "cyber" is a prefix to describe a person, a thing, an idea or a space being related to the computation.

The cyberspace, which internet is its very example, has gained a significant role in human life nowadays. Therefore, knowing it will help to resolve malfeasance related to this issue.

1-2- Cyber-Crime

After the existence of the cyberspace, some debates arose about cyber-crimes. Although some believed there is no cyber-crime and these kinds of crimes are the traditional ones which occur in a new method. As Grabosky said, cyber-crime is the same old wine, poured in new bottles [4]. These jurists believe that cyberspace is a new place to commit the crimes and all the so-called cyber-crimes are actually transformed traditional crime with a new method of commitment. This idea is based on this fact that the essence is the same; just the method is changed [5].

The second group of jurists believes that cyber-crimes are an independent sort of crimes. For example unlawful accessing to the data or systems or spreading computer viruses are only imaginable in cyberspace; therefore these should be called as pure cyber-crimes. Thus, the second opinion is based on classifying cyber-crimes to pure cyber-crimes and crimes committed in cyberspace.

In a different classification two sorts of cyber-crimes are differentiated. The first is cyber-crimes technological in nature, and the second sort is cyber-crimes with pronounced human element.

***Corresponding Author:** Mahmoud Malmir, Ph.D., Assistant Professor of Islamic Azad University, Khorasgan Branch, Isfahan, Iran. dr.malmir1@gmail.com

Cyber-crimes in nature have three major qualities: 1. These crimes are generally specific events from victim's viewpoint. 2. These crimes take place with the aid of bad wares as keystroke loggers and Trojan horses. 3. This aid could facilitate the vulnerability of the victim.

Cyber-crimes with pronounced human element have two major qualities: 1. these crimes are facilitated by some wares not classified as bad wares; like conversations between the users or file transfer based on FTP. 2. They are generally based on relations or repetitive events.

Actually this classification is based on the portion of using technology and the role of human in committing such crimes. In the first category, human malfunction does not have an explicit part and bad wares misusing the gaps of computers and software are the ground of crime. But the second category, the crime is the consequence of human act. In this case the systems and software might be intact, but the users make the unlawful situation.

In spite of these explanations, there is not a complete definition for cyber-crimes, and there are even some disputes about the title to be cyber-crime or virtual crime. We define cyber-crime as "any crime committed or facilitated by using a computer, network, hardware or software".

1-3- Organized Crime

The term "organized crime" first established in criminological texts. It was first used by Sutherland in his famous book "The Principles of Criminology" [6].

There are many explanations about organized crimes. We are going to mention some of these which are related to our discussion.

Article 2 of United Nations Convention against international and organized crimes in year 2000, known as Palermo Convention holds: an organized crime is a special or specific crime mentioned in convention, which is committed by a group of three or more persons with purpose of gaining financial interest, directly or non-directly, for a period of time.

Another explanation which is based on classification of duties and tasks, defines organized crime as: unlawful and cooperative acts of a group of persons with conspiracy for gaining financial interest or power, with using any criminal mean imaginable [7].

Nine different characteristics about organized crimes are as followings: 1- they have a grouped structure, 2- they have an initial central power, 3- they have a gradual nature, 4- existence of the tacit regulations for the members, 5- existence of professional criminals, 6- having organized operation, 7- responding to unlawful properties or services, 8- exclusivity and 9- using offensive methods. [8]. Nowadays there is a debate about official and non-official organized crimes among the criminologists, but Iranian legislation does not affect so forth.

After this introduction, we reach the principal issue of the research, which is the combination of cyber-crime and organized crime. We want to see if: A) an organized cyber-crime is imaginable? And if so, B) how Iranian statutes react against these kinds of crimes? And C) what are the preventive means of organized cyber-crimes in Iran?

These are the questions that are going to be answered in this research.

2- Possibility of the cyber-crimes

There are three different approaches about the possibility of organized cyber-crimes: All cyber-crimes to be organized, all cyber-crimes not to be organized and some cyber-crimes to be organized.

2-1- All cyber-crimes are organized

Some of the jurists think that a non-organized cyber-crime is not imaginable. They think that cyber-crimes are not committable by one person and any cyber-crime needs a specific amount of organization at least in one of its major dimensions [9]. The cyber-crimes committed in World Wide Web need team work; for examples a pornographic site needs contents, uploading, traffic control, etc. It is not possible for one person to do all these.

Although it should be noticed that some of these kinds of crimes may be committed by one person at first, and then through the membership and making a collaborative area the actions of the site is expanded.

But it seems that committing a cyber-crime only by one person is also imaginable. That means the idea of all cyber-crime to be organized is somehow wrong and cyber-crimes are not absolutely organized.

2-2- All cyber-crimes are not organized

On the contrary of the mentioned idea, another opinion held that a cyber-crime could not be organized, according to the nature of the cyberspace. It is said that: the nature of the cyberspace does not have accommodation with hierarchy; the cyberspace is a network. Networks are expanded, moving and dispersed, but organized crimes are hierarchic, vertical, rigid and stable [10].

These ideas describe the horizontal structure of the cyberspace as a reason of impossibility of committing the organized cyber-crimes.

But in official organizations, in which the government raise its part in cyberspace, the hierarchic system is organized and it has nothing in contradiction with being cyber or virtual; although, the hierarchic system in official and governmental organizations and the hierarchic system in criminal organizations are not comparable; while the official organization is a horizontal system with limitations in accessibility. That means in such system there is boundaries in rights and duties of the officials and no one has the absolute power. But in a criminal system, the leader has an absolute control on all of the elements of the organization.

It seems that this would be a wrong idea and the structure of cyberspace does not tolerate a hierarchic system, since this space is founded by cellular groups which do not have the ability of connection. This means that in criminal organizations also, there is no hierarchic systems like what is imaginable in actual world; however some sort of employer-employee relationship could be detected in between.

For a long time, there was an idea that all kinds of cyber-crimes are committed by individual hackers who are generally reluctant in working on a team [11]. But nowadays this has been confirmed that cyber-criminals are not generally isolated and sometimes they are social and normal persons.

2-3- Some cyber-crimes are organized

According to what has mentioned above, the two absolute ideas about cyber-crimes are not scientific and rational. This means that some cyber-crimes are organized and some are not. According to this idea the cyber-crimes are classified in two major categories: 1- cyber-crimes committed by actual or non-virtual organizations. 2- cyber-crimes committed by organizations affiliated with cyberspace.

2-3-1- cyber-crimes committed by actual or non-virtual organizations

About existence of traditional criminal organizations in cyberspace there is an opinion on which these criminal organizations find their way into cyberspace after development of this space and augmentation of the cyber relationships [12].

According to this idea, which is generally based on the criminological theory of transmission of spaces, the concepts crime, wrongdoer and victim are transmitted into cyberspace; although these concepts are somehow different from their mirror concepts in actual world [13].

It is said that organized crime is completely suitable for using cyberspace [14]. The emphasis of this idea is generally based on innovation and compatibility of informatics-operative and fleeing from knowing cyberspace which is a mean to facilitate unlawful actions of criminal groups. Therefore, the transmission of organized crimes from the actual and physical space to cyberspace is a common issue; because organized criminal groups always choose certain industries as their target, and cyberspace and e-commerce are some suitable goals for such groups.

An example for the actions of traditional organized criminal groups is stealing the 400 million dollar budget of European Union for Sicily by Mafia. It is an obvious example of actions of the biggest criminal organization of the world in cyberspace.

It is deducted that presence of organized criminal groups in cyberspace has two major faces: one is organized wrongdoing in cyberspace and the other is using the abilities of cyberspace in facilitating the crimes in actual world. The second function is more common and nowadays the principal task of cyberspace for criminal groups is facilitating.

The obvious example of this issue is seen in terrorism. Although some believe that terrorism is not an organized crime and some do, the organized aspect of terrorism is more imaginable. In many cases these groups use cyberspace as an informative mean. In the following we will discuss about these organized crimes.

Using this space has two methods. The first one is using informative systems for making connections between the troops and the second is using informative and publishing possibilities of cyberspace. One of major characteristics of terrorism is using media [15]. This approach has been used by some groups like Al-Qaida and this group has published the pictures and films of its terrorist attacks in cyberspace.

Cyberspace is a very convenient area for terrorist activities because:

1- Cyberspace being borderless: the trans nationality of cyberspace is a big advantage for this reason.

2- Reducing the cost of crime: in cyberspace reduces the cost of crime. For calculating the cost of crime, two aspects are considered: one is the result and another is the possibility of punishment. The cost of crime is a vital issue for the terrorists, because the crimes they are committing have usually severe punishments.

3- The possibility of making loss, without harming anybody: many terrorist activities in actual world are along with harming human beings, and that is not compatible with their goal to attract public. Physical harms, especially if accompanied with death, are making bad reactions; that is why the terrorists benefit the possibilities of cyberspace to commit crimes.

4- The easy supply of facilities of the terrorist activities: the terrorist attacks usually need facilities which their supply may have serious difficulties. According to these dangers and difficulties and the possibility of being arrested and punished, a few men may be able to perform such activities. The cyberspace supplies these facilities in a easier way and increase the chance of success. 3

5- The universal broadcasting of success: the media and cyber-connections are the most common tool which is used worldwide; therefore any malfunction in this system would easily ruin the credit of any state or organization. Since the terrorists are looking forward to broadcast their activities universally, this space may be the best choice. On the other hand, any failure will be unknown and won't harm terrorist's reputation.

6- The possibility of immediate and precise coordination: one of vital tools of terrorists is transmission tool on which they are able to transmit the information and inform each other of the situation. The cyberspace supplies the possibility of immediate transmission in audio, video and text. The terrorists use cryptography and steganography methods to hide their unlawful information.

2-3-2- cyber-crimes committed by cyber groups

The certain characteristics of cyberspace necessitate the study of organized criminal groups. Some of regulations about organized crimes in actual world are different from the organized cyber-crimes. In this issue, central power, continuation and using harshness which raise about actual world organized crimes have no place in organized cyber-crimes [16].

About not having used harshness by the organized cyber-criminal groups the European Council held that: cyber-crime needs less geographical surveillance, harshness, personal connections and official organizations than a traditional organized crime.

To confirm this issue, it should be said that organized structures and continuation of criminal groups have altered; therefore some have said that: these organized cyber groups which are the pioneers of cyber-crime, are some unstable, non-hierarchic groups that gather to commit a certain crime and then they abolish [17].

Criminal cyber groups are actually derived from their criminal micro-culture in cyberspace. The most important of these micro-cultures are hackers and crackers' culture which has criminal tendencies in between; although some of these hackers published charters about their ethical and humanistic virtues, but their activities usually harm lawful properties of the individuals. For example stealing a software and publishing it make important losses for the programmers and producers.

According to the situation of hackers' micro-cultures in constructing cyber-crime organized groups, it seem that getting to know these micro-cultures has a big role in knowing different aspects of these groups; because the foundation of many cyber-crime groups is based on hackers' micro-cultures.

Many characteristics which are traditionally related to organized crimes are compatible to the hackers and crackers too. This compatibility made some sort of natural relationship between two unlawful networks which is the translation of a new generation of cyber-crimes: organized cyber-crimes.

This point of view seems to be compatible to the reality of cyberspace, because many cyber criminals somehow experience a metamorphosis and look forward to financial benefits for their activities [18].

But some defensive improvements in recent years which increase the ability to confront hackers in cyberspace made the commitment of cyber-crime more difficult and make tendencies to new methods in crimes. These realities made the United Kingdom's bureau against cyber-crime announce year 2006 as the actual beginning of the cyber-crimes.

Organized groups for committing cyber-crimes are an undeniable reality; therefore their characteristics and aspects should be studied carefully to find ways of confrontation. For this reason, the most important characteristics of these groups should be considered:

- They are fluid and their members are changing all the time.
- They constitute to fulfill a criminal plan separately and abolish after the fulfillment.
- They are constructed by casual people who accept gross danger in exchange of little sum of money.
- They look at criminal plan on a childish way.
- There is usually no physical contact between operatives and leaders.

These characteristics should be chased only in non-governmental organized criminal groups. Nowadays, the concept of official or governmental organized crime is raised up among the criminologists and this idea is also emphasized in the case of cyber-crimes. The debate of cyber-army,

which is an issue in international relations, is an important division of organized cyber-crime. These groups, known as cyber-army, are only occupied with committing cyber-crimes and destructing the data of other countries.

3- Position of Iranian Legislations against Cyber-Crimes

After studying different theories about cyber-crimes, hereby we are able to conclude that organized cyber-crime is a sort of cyber-crime which could be committed by organized criminal groups in actual world or cyber-criminal groups in cyberspace. We discussed the general and international position of the jurists on this issue; now we will study the position of Iranian legal system.

The most important legislation about this subject in Iran is the Computer Crimes Code 2007 (1388 Hj).

3-1- Computer Crimes Code

Studying Iranian statutes shows reactions against organized crimes just in certain cases. In the present, article 14 and 26 of computer crimes code of 2007 mention organized crimes; although these two articles are about increasing the crime of the computer offenders. The notion of article 14 holds: if the offender mentioned in this article, do the activities as publishing, contribution, supplying or preserving pornographic data in financial and commercial purposes, in an organized way, will be sentenced to the both punishments subject to this article. This notion considered being organized as an increasing factor of the punishment.

Other legislation on this matter is the paragraph D of the article 26 of same code. According to this paragraph, being organized is an increasing factor for all of the cyber-crimes.

An important issue about this code is in neither articles mentioning the organized crime, this concept has not been defined and determined. The importance shows up when the punishment of the sorts are compared. If the judge considers the crime as organized, it could have lead even to death sentence, while if not, the punishment is up to two years of imprisonment.

3-2- Draft of New Islamic Penal Code

In the draft of new Islamic penal code organized crimes has been mentioned in a general way and according to not having define them carefully, some contradictions might be imaginable. In paragraph 2 of article 122-3 of this code, the crimes are divided into regular and organized; although the determination and difference of these two sorts seems to be forgotten by the authors.

To sum up, it seems that Iranian legal system suffers the lack of definition of organized crime, and organized cyber-crime is also not defined. The most important international document on this issue is the convention of international organized crimes and its protocols. Until now, Iran has not admitted the convention in the parliament; therefore, this sort of crime has no position in Iranian legal system.

The judicial power just would apply the general rules mentioned in different legislations to punish the committers of the organized cyber-crimes.

4- Conclusion

In the present research, it has been discussed that the cyberspace could be a host of various crimes which one of those is organized cyber-crime. The ideas on which the cyber-crimes are absolutely organized or absolutely not organized could not be true. The organized cyber-crimes are committed by either organized criminal groups of the actual world, with the purpose of facilitating their activities in actual world and expanding the domain of their crimes to the cyberspace, or, groups founded especially in cyberspace. The latters are divided into two major groups: the groups of hackers that may begin with political or ideological motivations and then shift to financial purposes. The other groups are officially defended and sponsored by the governments.

Knowing the cyber-criminal groups and classifications of those groups, could have an important preventive role. This issue should be considered by the legislators, while the general rules of computer crimes do not respond the necessities of this area. The separation of organized crimes in the actual world from the cyber crimes of the cyber groups' crimes has a significant preventive effect.

It should be accepted that cyber-crimes are a reality which is expanding in the globe and every moment cause more dangers and problems. Confronting these unlawful activities need the global cooperation; since the cyberspace is a borderless entity.

In Iranian legal system, there is no definition for either organized crime, or cyber-crime. It means that the determination of organized cyber-crime is also a difficult issue by the jurists and the judges. Although there are some general rules in penal code and computer crimes code, but it seem the legal

system needs an independent legislation about cyber-crimes to make confronting these kinds of crimes and criminals more possible.

REFERENCES

[1] Di Angelis, Jina (2004), Cyber-Crimes, High council of informatics, Tehran.P. 7.

[2] Golmohammadi, Ahmad (2006), Globalization, Culture, Identity, Ney Publications, Tehran. P. 39.

[3] Bear, Stanford (2005), What is Cybernetics?,Tadbir Monthly, No. 155. (in

[4] Grabosky, Peter (2007), The Internet, Technology, and Organized Crime, Asian Journal of Criminology, Vol. 2, No. 2.P. 243.

[5] Nisbett, C (2002), New directions in cyber-crime, http://www.qinetiq.com/home/security/information_and_network_security/

[6] NajafiAbrandabadi, Ali Hussein (2006), Discussions on Criminology, ShahidBeheshti University. P. 850.

[7] Shams Nateri, Mohammad Ibrahim (2001), Studying Iranian Criminal Policy against Organized Crime, with an Approach on International Criminal Law, TarbiatModarres University. PP. 23-24.

[8]NajafiAbrandabadi, Ali Hussein (1385 Hj). P. 939.

[9]Nisbett, C (2002).

[10] Ibid.

[11]Zarrokh, Ehsan (2009), Are Criminological Theories able to Determine Cyber-Crimes?, ITDiscussions, Official Journal Publications. P. 437.

[12] Brenner, W. S. (2002), How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina Journal of Law and Technology, Vol. 4, No. 1. P. 24.

[13] Zarrokh, Ehsan (2009). P. 117.

[14] Olson, J. L. (2004), The Threat of Systematic and Organized Cyber-Crime and Information Warfare, http://www.american.edu/traccc/resources/publications.

[15]JalaliFafahani, Amir Hussein (2006), Cyber Terrorisme, Law and Jurisprudence Review, No. 10.P. 89.

[16] Brenner, W. S. (2002). P. 45.

[17] Ibid. P. 47.
[18]Zarrokh, Ehsan(2009). P. 113.