Cyber Criminology

Written by: Abdolreza Tarzi – Iran

Email: rtatft@yahoo.com

Publisher:www.haghgostar.ir

Introduction

Criminology during its one hundred years of life was ever seeking for detection of crime-creating factors and conditions affecting the expression of criminal behaviors in order to achieve the crime prevention methods and offenders' treatment, improvement and training styles by means of all academic specialties.

Meanwhile the considerable point is that such an effort has been taken up to the beginning of 1360s and concurrent to emergence of cyber crimes only in the real world. Although there are some common points in the comparative studies of real space and cyber space, but cyber crimes have provided new studying gateways for the criminologists, because these crimes in their development trend not only have created the conceptual and evident challenge for the traditional penal law but has retained its specialized literature. However, some believe that reforming the traditional penal laws met the needs against cyber crimes, in return some other believe that the cyber world is a new world and cyber offenders as regard to the criminology are different from common offenders and require new punishments and treatments.

a. Definition of cyber criminology:

According to the definitions presented for cyber criminology and its comparison with the definitions presented for criminology so far, it is concluded that "cyber criminology is studying the crime occurrence in the cyberspace and its effects on the real world and course of actions for prevention such crimes". The objective studies on the cyber crime files show that making the virtual personality by non-identification mentality as well as convenience and extension of committing some crimes in the cyberspace has provided a prone context for emergence of personality and mental vacuums, thus we believe that the real personality of a cyber offender should be sought in his cyber personality; in other word, the virtual personality made by the cyber offender indeed is his same "real self" that he couldn't express in the real world due to the different reasons. So, as quoted by the French Professor Gaston Stephaney, "recognition of offender's personality" is considered as an important topic in the cyber studied.

b. Characterization of cyber offenders:

Analyzing the personality of such offenders indicates that they exclude somehow an abstract ability and cannot image and visualize the outcome of their behavior in order to have self-control in prevention from committing the crime in the cyberspace. Such individuals are affected by the present and conduct their behaviors without any calculation and contemplation. For instance, in a case the cyber offender only because of anger disabled the database of university website, moreover disturbed the computer system and made problems for thousands of students to register and attempt the course credits and excused his criminal action only as momentary anger and inattention to what may be occurred. In another case, the cyber offender while programming was encountered in temporary disconnection of internet service and due to the momentary anger hacked more than 10 thousand of related ISP users.
The cyber offenders despite of technical capability and high intelligence are unable people and by seeking refuge to cyberspace cave try to compensate the deficits but they fail in this refuge and exit from their artificial refuge ad so called show themselves up. Probably aiding this fact, the cyber crimes prosecutor institutions are able to identify the cyber offenders within the short time despite of cyberspace complexity.

c. An overview on cyber crimes:

The titles of cyber crimes according to the Computer Crimes Law of Islamic Republic of Iran ratified in 2009 are as follows:

1. Unauthorized accessibility to the computer or communication data;
2. Unauthorized listening to transmitting content in the computer or communication data;
3. Unauthorized accessibility to the transmitting the secret data in the computer or communication data or data carriers or its achievement and listening;
4. Providing the transmitting the secret data in the computer or communication data or data carriers to the access of disqualified persons;
5. Disclosing or providing the transmitting the secret data in the computer or communication data or data carriers at the disposal of government, organization, companies or foreign group;
6. Breaching the security policies of computer or communication systems in order to access the secret data transmitting in the computer or communication systems or data carriers;
7. Unauthorized change in the reliable data or fraudulent creation or entry thereof;
8. Changing the data or signs available in the memory card or processing in the computer or communication systems or chips, or fraudulent creation or entry of data or signs therein;
9. Unauthorized deleting, destroying, disrupting, non-processing the other data of computer or communication systems or data carriers;
10. Unauthorized disabling or disrupting the computer or communication systems;
11. Unauthorized blocking for access of authorized users to the computer or communication data or systems;
12. Unauthorized stealing the data belonging to the others;
13. Unauthorized acquisition of property via computer or communication system;
14. Publication of vulgar and obscene works via computer or communication system or data carriers;

15. Facilitating the accessibility of vulgar and obscene contents to the people via computer or communication system or data carriers;
16. Desecration through publishing the others' deviated audio and video via computer or communication systems;
17. Propagating the falsehoods via computer or communication systems for hurting the others or disturbing the public;
18. Avoiding the filtration of criminal contents by the service providers;
19. Unauthorized use of international bandwidth based on the internet protocol for establishing the communications;
20. Producing, publishing, distributing or transacting the data or software or any other electronic tools used merely for the purpose of committing computer crimes;
21. Selling, publishing or accessing the password or any data that provides unauthorized accessibility to the computer or communication data or systems belonging to the others;
22. Training the styles of committing the crimes including unauthorized accessing, unauthorized listening, and computer spy, disrupting the data or computer and communication systems.

d. Cyber criminal etiology

Plenty of causes and reasons such as economic, cultural and political factors, mental and psychological problems such as depression, anger, jealousy, revenging, hating, recreation and entertainment, inferiority complex, inferiority, sense of competition are effective on the formation of cyber crimes as follows:

1- Economic crimes:

Crimes such as unauthorized acquisition of property via computer system or the same swindling is a sample of such crimes which are majorly committed with the economic purposes; for instance some cyber offenders access to the banking account information of users through fishing or entering the passwords and other information available in the related systems and so withdraw the funds from peoples' banking accounts.

Moreover, in many cases, the computer crimes that apparently are not economic are committed with the economic motivations and vice versa some apparently economic cyber crimes are committed by noneconomic motivations; for instance in a case, the individual after accessing to computer system of his victim and achieving his personal documents and evidences, tried to extort him. Vice versa, in another case, the accused has penetrated to the banking account of one of bank clients only for expressing his capability in hacking and took an amount and refund it exactly to the bank in order to show lacking the banking network security and his high capability in this field. It is interesting that he explained the cause of his criminal behavior so: "whereas I was seeking for a job, intended to show my capability to the others in order to provide the requirements for employment!!"

2- Cultural crimes:

Cultural poverty and non-binding upon the society values and religious beliefs are considered as the important causes for committing some crimes in the cyberspace. As mentioned above, upon creation of

cyber world, many barriers have been removed and crime commitment has been facilitated. Cyberspace has provided the conditions for the offenders to commit crime in spaces excluding where the outcomes and effects of their actions are appeared therein, and conveniently and with the lowest cost and anxiety occur the maximum losses and damages and yet remain unknown. Committing the crimes such as propagating the vulgar and obscene works via computer or communication system or data carriers, or facilitating the people's access to vulgar and obscene contents are deemed as the cyber crimes that inattention to the morals and society values leads thereto. Establishing the immoral websites and promoting the sexual promiscuous and unhealthy relationships between the girls and boys as fried-finding sites, online immoral films distribution sites etc. are considered as such crimes.

3- Mental and psychological problems:

The major part of computer crimes committed in our country (Iran) is arising out of mental and psychological problems of cyberspace offenders. A man has propagated his wife's personal photos and videos in the internet sites only because of dispute with his wife and for the purpose of revenging her. A woman has propagated her unveiled photos in the internet in order to only revenge his husband that has remarried. In another case, a man out of jealousy has installed the listening software on the computer of a woman and so received the texts of her personal chats and sent to the others. In other cases, the individuals by making the fake pages in the social websites dishonored and affronted his victims.

The samples of this part of cyber crimes committing causes are more extensive than other causes and reasons and require criminology studies in this context.

e. Cyber crimes victims:

Cyber crimes victims are indeed the victims of technology development but the notable point in the meanwhile is that many of cyber crimes victims express considerable talent for victimization and are victimized by the cyber offenders easily. Some internet defrauds by means of obtaining the information through very simple channels and misusing the personal photos and secrets are samples for this topic. We believe that the victim of cyber crime is not ever innocent and maybe own the beginner of cyber offense inadvertently.

Personality weakness, lack of sufficient information in relation to the cyberspace and inattention in preserving the data etc. are deemed as cases that helps the cyber crime victim in his victimization.

f. Preventive criminology in cyberspace:

At the end of this discussion, it is concluded that the loss incurred by the cyber crimes is more extensive and non-compensable than traditional crimes. The objective study on cyber crimes demonstrates this fact that in the most cases, material, moral and psychological losses are incurred to the victim. On the other hand, the specific nature of cyberspace requires cyber prevention seriously. Promoting the level of society's information on cyberspace and informing of cyber crimes and confronting strategies, promoting the religious and moral beliefs particularly among the juveniles and youths are assumed as the course of actions for prevention from crimes formation in cyberspace.