Criminological analysis of fraud in cyberspace

Alireza Akbari
MA student of Criminal Law and Criminology, Department of Law, Rafsanjan Science and Research Branch, Islamic Azad University, Kerman, Iran

Seyyed Mehdi Ahmadi Mousavi
PHD of Law, Assistant Professor, Department of Law, Rafsanjan Science and Research Branch, Islamic Azad University, Kerman, Iran

Abstract

Information and communication technology in the late twentieth century the early twenty-first century, great progress with the development of cyberspace is strictly social welfare has brought to mankind. So individuals and organizations has moved to this space. This has caused, opportunities and create new means for crime and criminal activities to be transferred there.

Including new crimes committed in this area is fraud that is now in the classic definition, a new alternative is developed in cyberspace as a "cyber fraud" be interpreted. Therefore, this study investigated the factors causing crime prevention information and communication technology and it seems to be necessary.

The aim of this study is criminological analysis of cyber fraud. It is obvious that proper and effective utilization of the space provisions is a violation of their norms can lead to damages and some of them is a crime. Since the occurrence of fraud in cyberspace is possible, and sometimes obvious and the hidden characteristics of a criminal act in such a criminal act is the identity of the offender and the ease of implementation, We can say that the lack of written laws as well as the lack of appropriate sanctions and penalties are disproportionate prevalence and frequency of these crimes are crimes in cyberspace.

Keywords: input, crime, cyber space, scams.
Today, many people from the global network or the Internet to exchange messages or other activities they use. These networks are destroyed in time and space and put too much power in human hands. Because of this shared space technology and new concepts such as the rule has manifested cyber and so on. Cyberspace as well as other elements of social life, from being a very flexible and parcel of the social phenomenon called mass spared. In general, it is today known as cybercrime, two categories of offenses: The first group are crimes like there are in the physical world and cyberspace without changing their criminal elements, with features that puts in the hands of criminals, facilitates crime. Crime coverage of these fields are quite large and international crimes such as terrorist acts against national security and even to crimes against property and persons in the fall.

Computer fraud includes crimes that with the advent of information technology into specific criminal law and the principles and rules governing the traditional fraud is challenged. Cyber crooks of the nominal and the result of the mass resembles the traditional fraud. But differs from the process of constituting the offense would have been committed and Nasser specific cyber crooks as a crime to be considered independent of the classic fraud. Note that any committing fraud by computer, cyber crooks are not considered. This paper is a small glimpse into the field of crime and fraud, cyber Street and the aspects to be investigated.

**Types of cybercrime**

Cyber-crime or general categories can be placed in four categories. A) Classic description of cyber-crimes: crimes assign fall in this category are considered to be traditional crimes, but now due to technological progress, with new means done. Among these crimes can be cyber fraud, forgery, cyber, cyber destruction, cyber espionage, and more. B) offenses against the confidentiality of the data system: Each symbol of topics, concepts or instructions, including text, audio or image processing for communication between computer systems used by a person or a computer system and is created by the computer system, said data content. C) Crimes against data integrity and system accuracy: Change, create, fade or stop the computer and telecommunications for the purpose of fraud, non-use, destruction or disruption of data or electromagnetic waves, preventing the achievement of those authorized to Change the password or encryption of data among the crimes that are placed in this category. D) Crimes related to content: This category of crimes under its inclusion puts in their computers as tools used by criminals to commit crimes and not merely information technology field provides committing them. For example, the publication of pornographic content such as displaying or showing the sexual organs of male and female human sexual intercourse, promoting or inciting or encouraging sexual perversion or suicide via computer and communication systems fall into this category.

**Foundations criminalize cyber crooks**

According to the jurisprudence as a punishment for possession of the property, John, member, freedom and reputations of others is, then, a kind of guardianship over the other and it is the nature of man to other provinces unless definitive proof that it also be present.
This legislators and widespread arbitrary criminalization of behaviors are prohibited and require that they limit criminalization to cases that a behavior will lead to severe injury or blame. Criminalizing any kind of intervention and restriction of rights and freedoms of individuals is studied (Shamsi Nateri et al., 1390). In other words, it is to prevent increasing criminalization in total autonomy and (increase) the dignity and repute of citizens (Nobahar, 1387).

In cyberspace due to specific features such as ease of crime and technology freedom in this space, potential for more criminal phenomenon is undesirable because one of the characteristics of a distinct and yet is valuable than other information technology and electronic communication technology (Jalali Farahani, 1389). As a result of this crime in cyberspace is also very convenient. Anyone with a computer that has Internet connectivity to computer literacy and familiarity could be potential criminals (Fazli, 1389).

In fact, "a comprehensive identification of possible risks posed by cybercrime various aspects of social life, a prerequisite for the successful implementation of the law in this area is good legislation" (Javan Jafari, 1385).

However, in most advanced countries in the field of data processing, the use of cyberspace with high-speed international bandwidth and making use of such communications is accepted as a right of citizenship (Elahi Manesh and Sadreh Neshin, 1391). If the legislation criminalizing behavior that is not cause enough damage and blame will undermine the rights and freedoms of individuals and people actually will disobey orders legislators determined to refrain from committing such behavior, the use of the Similarly, Circumvention of the refusal by the graph.

**Basics of criminology cyber crooks**

Durkim, the French sociologist believes that any action that is worthy of punishment is a crime, in other words, any act or omission that order, peace disrupt social peace and the law have to determine the penalty for the "crime". In Durkim's view, "We work for "Crime" was convicted but also because it criminalizes is condemned" (Sotoodeh, 1382).

In expressing the common character of all crimes write: "Crimes are acts that all members of society in general condemn them" (Parham, 1369). If it is proven fact that a histo-pathologic findings. The reality is that crime, all criminologists agree with this point. (Kuzer and Rosenberg, 1378). Investigation of crimes, is regardless of cultural and civilizational characteristics of criminologist's point of view unprofitable, because the crime was related to culture and civilization and is not a function of time and place. Durkim believed that society existed before human and their effect on the accumulated and trained is fluent. The spirit of each individual is directly related to the constitution and functions and commands and social patterns and the factors of influence for their private relationships "(Taj zaman, 1364).

Durkheim and society in general scientists believe that the phenomenon of delinquency crime cannot be explained by psychological factors and many people because these factors have important role in the delinquency individuals but social factors such as family conditions and limitations of affection, parental discord, divorce, parental criminality, unemployment, immigration, the media, the lack of religious beliefs, political factors, war and bad economic
situation is family important and decisive role in the delinquency and criminal acts of individuals (Najafi Tavana, 1377).

In general, look sociology, criminology interpreted as a move away from the values and rules of society that appears in various forms and dimensions.

Investigate the causes of fraud in cyberspace

Today, we face the real world with a virtual world that has three major characteristics: the rigidity and flexibility of the elements of the offense in time and space, virtual space perpetrators relative anonymity that in fact crime is difficult to identify them and place and a world without crime range that allows criminals to crime out of the place or from around the world to do (Najafi Abrandi Abadi, 1390: 13).

In this article, the main focus on the overall causes of crimes ranging from traditional and cyber placed in explaining the causes of the specific characteristics of cyberspace as a special variable and determines, will be considered.

(A) Personal reasons effective computer fraud

Sex, age, cynicism, arrogance, selfishness, hatred, revenge, madness wealth, moral insanity, aggressive, impulsive anger, revenge, beliefs or specific tendencies of individual factors is due to bio-psychological situation, he tends to do contrary to the norm of behavior. For example, what about the age of the perpetrators of cybercrime as one of the causes considerable personal, financial crimes and offenses against public morals and ethics in the elderly as in younger people? In fact, teenagers accounted for a large share in the second crime. Teen person after entering the stage of maturity with changes in physical, mental, and your character is facing these changes and an attractive and accessible environment as a virtual world he is leaning toward this new world.

In this regard sexual abusers are using cyberspace to be able to upload and distribute high volumes of pornography issues, the groups are identical with thoughts and ideas and then quickly provide Internet services to groups. Prostitution and sexual abuse among children and adolescents in the real world convert (Goodman and Brenner, 2010).

Today, children and adolescents with access to cyberspace with an infestation of advertising, film, photos, stories and characters that are familiar with this situation with its positive effects, also has brought negative effects. So societies to reform and correct training of the next generation have always dealt with these factors. What is the cause of children as young as vulgar and obscene contents notably, the age, desires and values demanded in this segment, the appeal of these contents and lack of alternatives is legitimate.

So, people at an early age due to the particular circumstances in which are placed by environmental factors. Therefore, preventive measures and alternative forecast legitimate and interesting may be helpful in this regard. Another person who shaped the causes of crime is particularly cybercrime, mental and personality characteristics of individuals. A moral insanity or madness or anger or vengeance instant wealth each process in turn speeds up their crime.

Thus, as is clear from the examples of individual causes of some mental and personality characteristics of the environment affected by the tendency to commit cybercrimes is one of
the main causes that although the nature of cyber-crime measures, which are further tolerance is reason. Cybercrime is a glaring and entertainment from other causes which, in most cases, merely to demonstrate your abilities and talent perpetrators of these crimes are, in such a way that the hacks are access to the data a site or misadjust of the other or the desirable and proud to be seen which of course has its own problems to deal with such people there (Varvayi and Momeni poor, 1393).

(B) Effective social causes computer fraud

Cultural status of the individual and the community, family and peer group environment in which one lives, economic status, lack of belief in the norm, the activities of mass media etc. including social factors that person's tendency to commit crimes, particularly cybercrime, are very effective.

In this regard, the most important factor presented herein.
- Effective cultural survival in computer fraud
- Economic conditions affecting the computer fraud
- Computer fraud affecting poor families
- Effective opposition peer computer fraud
- The role of effective cyber victim computer fraud

Explanation of effective preventive strategy to commit fraud

In a general classification, theoretical and applied criminology is divided into two categories. Criminology your application is divided into three main categories: 1. Criminology Law, 2. Clinical Criminology 3. Preventive criminology.

After World War II criminology preventive and coincides with the United Nations human rights raised in the era of widespread general rejection of criminal law from the perspective of human rights. Several definitions of the concept of prevention and its characteristics are presented.

In one definition, Morris Cushion Canadian criminologist prevention: the definition stated: "The set of measures and specific measures aimed at curbing crime Non coercive, reducing the likelihood of crime and reduce the severity of the crime be taken on the causes of crime" (Ebrahimi, 1390).

According to the definition of prevention has been made, generally we can reckon a few essential traits for prevention: 1. Non coercive of measures 2. The specificity of the measures 3. To reduce the effects of crime 4. Taking into account social and environmental risk factors

Among the different classifications that have been made regarding preventive measures three types of social prevention, situational prevention and specialized prevention are more acceptable. For this reason, the study of prevention of cybercrime classifications used.

Before turning to the details of these three types of prevention, appropriate to the resolution of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders at the thirteenth session of the United Nations by the General Assembly in the form of Resolution number of 45.121 was approved, is noted. In this resolution, member states have been asked that, if necessary, by considering the following factors intensify their efforts in the fight against computer crime:
1. Modernize laws and criminal procedures.
2. Privacy promote preventive and computer security.
3. Selection of ways to sensitize the public and the judiciary and law enforcement to this problem, and the importance of prevention of computer crime.
4. Giving adequate training to judges, officers and those responsible for the prevention, investigation, prosecution and adjudication of economic and infrastructural crime.
5. Detailed studies in collaboration with interested organizations about ethical rules related to computer use and extend these rules as part of teaching and learning materials informatics.

It should be noted that resort to preventive measures, the justification for disrupting public security and freedom will not be considered. Therefore, persons with privacy these measures should only be taken for the prevention of cybercrime and the provisions of Article 12 of the Universal Declaration of Human Rights should always be considered.

The substance "No one's private life, family, home or correspondence shall be arbitrarily interfered and attacked the honor and tradition, everyone has the right to be supported against such interference or attacks."

**A social prevention of cybercrime**

This type of prevention is generally divided into two categories: prevention is community-based and growth-oriented. In this study, regardless of the classification of the general social environment and personal to provide preventive programs are discussed.

1. Institutionalize the culture of proper use of Cyberspace
2. Intervention in education process
3. Family-oriented measures
4. Victim's relaxation
5. Legislation up to date and efficient
6. Public Information

7. Fix economic problems

Situational prevention is the "changing of circumstances and conditions that it is high likely to commit crimes in order to make it hard, dangerous or attractions is dehydrogenation of crime. In this type of prevention, pursued with the conditions and circumstances that a reasonable person in the circumstances, it may be a crime to change his hand. Therefore, in relation to cybercrime as possible should apply strict security measures within this space, so that people's tendency to commit a crime can be prevented.

In this regard, in order to prevent the situation from cybercrime, measures should be grouped around three axes: first, increasing the risk of committing cybercrime, second and third increase crime problems, reducing the benefits of crime.

1) The cyber police
2) secure cyberspace
3) increased risk of crime
Conclusion

Cyberspace as a wonderful phenomenon, which developed in a short time of the coming revolution in human life has to foot, with all the functionality and complexity that it, like other human achievements, but also have negative effects. This means that the technology, of committing criminal acts exquisite and very improvements that have already been provided to any feasible way and was now in the hands of criminals and oppositional it as an opportunity to commit criminal acts is used.

Today, to be sure, not be removed from the list of ICT human life and not to its full glory of being criminals trying to mislead possible and it remains the only way to reduce the problems and obstacles facing human society is the most basic appropriate measures to identify the causes of cybercrimes is to investigate the mechanisms governing this space is blocked pathways to commit cybercrime. In this regard, special attention to developing preventive measures other than criminal and restorative justice rather than criminal justice and punishment useless is very important. In this regard, special attention to the principle of non-criminal prevention of crime, including social and situational recommendations offered that it is hoped that with the implementation of these measures and the development of scientific research in the field of cyberspace, we have seen a reduction or eradication of cybercrime.

1- The traditional system of criminal justice, it is important to respond to crime rather than prevent them. In this situation there is little background, crime prevention through social development, promising supplement for the current penal system. In addition, crime prevention through social development has many benefits and potential benefits such as savings in financial resources. For example, the United States Committee for selection of children, youth and families, estimates that a dollar invested in research to improve the quality of pre-school education is 4.75 dollars.

The preschool participants are much more likely to succeed in school and in their jobs and less likely to need public aid or commit crimes (Haward, 1383).

2- Some offenders for cybercrimes are perpetrated instantly and without elevated decision. Therefore, situational prevention measures applied on the Internet in connection with such persons will have the desired results.

3- Chase, prosecution and prevention of cybercrime involves training professionals, and is equipped with the latest technology of the day. Of course, they have the ability to continually update their keep. Otherwise, do not be too serious to deal with these kind of crimes had hoped. Such crimes cannot be prosecuted and research in the physical world had hoped. It is important here, to trace cyber criminals in this space and positioning them correctly.

4- Unfortunately, due to the trans-boundary nature of cybercrimes, law enforcement face challenges. Therefore, if the effective result of their actions, they must as soon as possible in accordance with international and regional treaties and documents available, as well as initiatives that can have in this field, the field of international engagement with the other enforcement provide.

5- The authorities have stated that the fact that law enforcement officials need to learn as much as technical issues are not cyber space. But obviously if it is judged appropriate to take
action on cybercrime, are relative to the nature of the space and issues related to this type of crime.
Classes specialize in this area closer to the specialization of courts and investigation of these crimes take, is recommended.
6- Defining concepts related to cyberspace, paying particular attention to the results of its survey, education and public awareness, review existing laws and regulations and laws efficient and predictable institutions to provide expertise in cybercrime and develop a general policy in the field of research resources, training, and research how to prosecute cybercrime and assistance in gathering evidence for similar crimes, among other measures to be taken in this regard.
7- Part of the way to deal with crime in cyberspace to create a culture of using computers and awareness of individuals and organizations about the dangers of computer systems and permanent monitoring of computer systems based on security measures such as physical security, personnel protection, protect communications and information protection against computer fraud is of particular importance. Given that involve computer crimes committed in the place where the result is not a crime as well as with respect to cross-border aspects of computer crime and the authorities in the area of the geographic boundaries of the Limitation. In this regard the need for international cooperation in the field of detection, prosecution and extradition stressed.
8- Free prevent identity-based tracking to track the invaders, criminals and fraudsters use cyberspace to the realm of criminal activity to be tight for them. To control and monitor virtual space through various means including Internet service providers monitor and control and monitoring communication networks, the prevention of crimes in these centers.
- Cyberspace was enjoying the activity and motion detect and prosecute is doing and problem affecting this manner, subject to suitable software to automate the design and implementation of it.
- Collect electronic argue a crime on the Internet and all the places where cybercrime occurs, since identify similar criminal acts in the future and identify the perpetrator or his footprint and utilizes technical analysis, digital argue a review of Preservation and collect evidence at the crime scene is effective in reducing cybercrimes.
- Evidence-based prevention of the crime scene on the Internet in terms of things like identify similar criminal acts in the future and create a database of offenders and reduce crime in cyberspace, cybercriminal techniques influence.
References


Ebrahim, Sh, 1390, crime prevention, Volume I, Tehran: Publication of, first printing.


Fazli, M., 1389, criminal responsibility in cyberspace, Tehran: happy, first printing.


Jafari, M., 1387, Concise criminology (summary of the topics taught criminology, Dr Najafi Abrndabady).


Javan Jafari, A., 1385, cybercrime and new challenges penal policy, the Proceedings of the Conference on globalization challenges its rights, Mashhad, Ferdowsi University.

Najafi Abrandi Abadi, A., 1390, from criminology real to virtual (preface criminology; Zhorzhpika), Tehran: Legal Foundation degree, second edition.

Nobahar, R., 1387, supported by public and private areas of criminal law, publications forest.

Shams Nateri; Abolmaali, V, and Alizadeh, Z., 1390, features criminalization light of documents and human rights standards. Quarterly strategy, the twentieth year, No. 58.

Varvayi, a, Momeni poor, H., 1393, cybercrime: the etiology and prevention.