Journal of Business and Social Science Review
Issue: Vol. 1; No.7; July 2020 pp.79-84
ISSN 2690-0866(Print) 2690-0874 (Online)
Website: www.jbssrnet.com
E-mail: editor@jbssrnet.com

Criminological analysis of Cybercrime from the Perspective of Prevention

Amin Amirian Farsani
Assistant Professor of Law, Shahid Ashrafi University of Isfahan

Mahmood Malmir (Corresponding Author)
Associate Professor, Department of Law
Khorasgan Branch
Islamic Azad University, Isfahan, Iran

Masoud Heidari
Assistant Professor of Law, Khorasgan Branch
Islamic Azad University, Isfahan, Iran

Abstract

New crimes can be new forms of old crimes, and they can be unprecedented crimes that may only occur in cybercrime. Has a 100-year history and in fact, it seeks to discover the crime factors and the conditions for the occurrence of criminal behavior by using it and, of course, taking advantage of all the specialization of scientific prevention by means of the methodology of crime and methods of treatment and rehabilitation of the perpetrators But the remarkable point is that such a trick was, by the early sixties, and at the same time as the emergence of cybercrime was merely in the real world, although there are common points in the comparative studies of the crime of virtual and virtual space, one can say: (Cybercriminology studying the causes of crime in cyberspace and its effects on the real world and prevention strategies for such crimes). The objective studies of cybercriminal cases show that the creation of virtual personality with the mentality of non-identification and, of course, the ease and breadth of committing Some delinquents in cyberspace provide a suitable platform for personality and mentality, but, irrespective of theoretical knowledge and criminal response in this regard, it is necessary to consider the criminalization of this criminal phenomenon as a criminological challenge, which must be addressed. In the light of technical criminology, the view is made on the developments of the time and the provision of land Not committing crimes against humanity for most of the knowledge and basic research in this field be organized.

Key words: criminology, computer crime law, cybercrime, computer crime, delinquent, victim

1. Introduction

In the course of its 100-year lifetime, criminology has always sought to discover the criminal factors and conditions for the occurrence of criminal behavior, in order to achieve it, and, of course, to use all the scientific expertise in methods of preventing crime and methods of treatment and rehabilitation of the perpetrators. But the remarkable point is that such a trick was until the early sixties and at the same time as the cybercrime came about only in the real world, although there are common points in the comparative studies of virtual and virtual space crimes. It should be noted that cybercrime has created new study boundaries for criminologists, since these crimes, in their evolution, have not only created a conceptual challenge to traditional criminal law, but also have their own specialist literature. However, some believe that the reform of the law Traditional criminal is responsive to the needs of cybercrime. In contrast, some believe that the virtual world is a new world, and cybercriminals are different in terms of criminology from ordinary criminals and require different punishments and treatments.

2. Problem statement

Today, all aspects of human activities are influenced by information and communication technology. In addition to individuals, governments, industrial, commercial, and ... industries have also been exposed to IT developments and have benefited from it.

Computerization is significant in all respects, from corporate affairs, industries, economic organizations and hospitals to government, all influenced by the rapid growth of information and communication technology. Medical treatments, air traffic control, storage of political, social, economic, personal, communications, etc. are all under the umbrella of this technology. Although the computer has made it impossible to interpret it, it can be viewed as a negative aspect of the crime, and some of these crimes are carried out on a large scale, which is unimaginable before the advent of technological information.

Would have Accordingly, computers and computer networks are increasingly being used as tools to help commit many "traditional crimes", such as scams, drug trafficking, terrorism and other forms of organized crime. These crimes are not specifically related to computers, but information technology is more and more used to commit them, for example, in order to establish secret communications in financial transactions and encryption of key information. This is particularly true of the Internet, which has created a "cyber space", where new forms of crime have emerged.

Changes in information technology, as mentioned, have led to the emergence of new forms of crime. At the same time, these changes and the new criminal forms resulting from it forced the legal systems to adapt to these developments. Given the vulnerability and vulnerability of hacking computer networks and the reliance of countries to these networks, disrupting or disrupting their systems can bring them back irreparable blows to the point where even the collapse of governments May also be due. Therefore, to facilitate the exchange of ideas and cooperation on the development of a culture of security between the government and the private sector at the international level, governments should work together to approve adaptation laws for cybercrime crimes. To this end, numerous measures have been taken to counter computer crimes in the area of international organizations and institutions, the adoption of the Budapest Convention, the recommendations of the Committee of Ministers of the Council of Europe, the Declaration of the International Criminal Law Association and the Congressional Assembly The United Nations Convention on Crime Prevention and Criminal Justice, including internationally and in the criminal justice system of Iran, first in the form of a computer crime bill in 2005 and, finally, the adoption of a computer crime law in 2009, including criminal acts It was like cybercrime.

Cybercrime requires specific criminal offenses, in addition to general principles, due to features such as the ease of committing a crime, the plight of the victim and the under-age of most of its offenders. Criminality in cybercrime is correct and acceptable on the basis of principles such as "necessity" and legitimacy, and while respecting privacy and citizenship rights, there is a fair proportion between criminal behavior and the type and amount of punishment, and at the same time, the tool And the available instruments of the criminal justice system and the vulnerable strata. From this point of view, it should be noted that Iran's criminal lawmaker, under domestic and international pressure, has adopted and drafted a law that more than copying and patterning more than cyberspace, criminals and victims, and legal challenges in Iran. The final and edifi cation of the Cyber Cybercrime Convention in Budapest, Hungary, and this legislator's thought takes the power of protecting the victim and victim of cybercrime in the afflicted issues and is limited to a few specific crimes.

On the one hand, the conventions and the international treaty, on the one hand, and the emerging crimes in cyberspace, on the other hand, make the legislator a criminal offense, but it has to deal with this issue on the basis of specific criminal and criminological components in order to be able to The correct approach has been put into committing crime and the concern is to what extent Iran's computer crime law has been consistent with this matter. It should also be acknowledged that one of the major branches of criminology is criminology, hence the guaranty We analyze the steps required in the computer crime law in order to determine how much the performance guarantee is based on the learner And objectives of the punishment. The Computer Crimes Act, as the first law in the field of criminal liability of legal persons, deals with the criminalization and punishment of legal persons, while it should be determined whether this criminal responsibility of legal persons has been affected by criminological and criminal offenses. Or that only an example has been made without regard to the foundations and approaches of Iranian law. One of the most important actors and actors involved in computer crime is that we are seeking a computer crime law that has the potential and the capacity to protect victims of the crime from a criminal offense.

3. Specific objectives of the study

1- Analysis of computer crime law from the perspective of criminology
2- Failure to guarantee legal acts based on the provisions of criminology

3- Understanding computer crime law from the perspective of supportive genealogy

4. Research method

The full description of the research method is based on the purpose, type of data and method of the descriptive-analytical research method.
Research hypotheses
1. The foundations of crime criminality are based on criminological components
2- The guarantee of the implementation of Iran's computer crime law is not based on the teachings of criminology.
3. The Iranian Computer Crime Act does not have the potential to provide the victims of the crime

5. Background research

The development of computer and telecommunication technologies has led to the realization of a new generation of crimes, which itself has a specific mechanism and framework that should examine its features and then provide a solution; the most important element is the examination of the fragmentation of these crimes and their actors. . This new generation of crimes is such that their legal analysis must be accompanied by technical analysis; hence the present paper addresses the specific aspects of criminological crime. In order to achieve this goal, the historical course of virtual crime, applicable legislative policies, the identification of elements of virtual crime, its perpetrators and its perpetrators, as well as the study of criminal theory in this space and their criminological analysis are necessary. With these interpretations, in order to write the present text and achieve these goals, we have used the analytical-statistical methodology and the library studies. As a result of this writing, we conclude that cybercrime is categorized in two main stages (before and after the establishment of the World Wide Web) and there are virtual organized crime groups. We examined cybercriminals according to their characteristics and features of cyberspace, and the best way to defend them based on the light theory of everyday activities should be precautionary prevention (Dindar, 2010).

Crime means action or refrain from action that opposes the order and peace of the community and is punishable in that sense. New crimes can also be new forms of old crimes, and they can be unprecedented crimes that may only occur in cybercrime. It has a 100-year history, and in fact it seeks to discover the crime factors and the conditions for the occurrence of criminal behavior, and, by the means of it, and, of course, to take advantage of all the specialization of scientific prevention in the form of crimes and methods of treatment and rehabilitation of delinquents But the remarkable point is that such a trick was, until the early sixties, with the emergence of cybercrime just in the real world. Although there are common points in the comparative studies of virtual and virtual space crimes, one can say: Criminology Criminology Study of the causes of crime in cyberspace and its effects on the real world and its solutions. Prevention of the crime is such a crime). The objective studies of cybercrime cases show that the creation of virtual personality with the mentality of not recognizing and, of course, the ease and extent of committing certain delinquencies in cyberspace provides a suitable platform for the occurrence of personality and psychological failures, however, regardless of theoretical knowledge and criminal response in this The field should necessarily consider the criminalization of this criminal phenomenon as a criminological challenge, which must be recognized in the light of the technical criminology of contemporary developments and the provision of a criminal offense against human beings, and fundamental research in this field Organized (Bayat Poor, 2015).

Criminal policy involves a coherent and integrated set of legislative, judicial and executive measures in the field of substantive and criminal law, and, taking into account the principles and standards of fair trial and respect for human dignity, seeks to provide timely and optimal proof of crime , To apply appropriate criminal responses in order to reduce the crime rate. Regarding some crimes due to the characteristics of offenders, the perpetrators and the crime of committing necessity, different measures should be taken against other crimes in order to allow for the detection and confirmation of crime and punishment and the appropriate provision of education and training. This distinct criminal policy for disregarding some of the basic principles and standards of criminal law or their bill and expansion is a differential criminal policy. Cybercrime as a handful of emerging crimes, because it selects cyberspace as a subject or a crime, requires this differential criminal policy for various reasons. The thesis attempts to elaborate a differential criminal policy for cybercrime, based on the significant differences between these crimes and traditional crimes, including the difference in the nature, manner, scope and context of the crime, the dangerous and dangerous difference between perpetrators of cybercrime, the explanation

And then identify and identify the types of this differential criminal policy with a descriptive and advisory approach within the scope of these crimes, especially within the framework of the requirements of the Iranian criminal system. The result of this study is that the logic of criminal law and the form of cybercrime are in many cases different from traditional ones, and thus it is necessary to formulate a coherent policy of crime against cybercrime in Iranian law. The effectiveness and effectiveness of the laws adopted to combat cybercrime requires a different look at issues such as crime definition, crime packs, criminal responsibility, criminal jurisdiction, preliminary investigations, and the way to handle and so on.

Although the Computer Crimes Act of 2009 and the Criminal Procedure Code of 2013 have significantly moved in this direction, it needs to be further developed and further developed, and especially requires the development of transatlantic judicial relations and assistance and the recruiting of international institutions in confrontation. With this category of crimes (Karami, 2015).

A relatively new technique of criminal profiling with the participation of criminologists, psychologists, and law enforcement officials seeks to depict the potentialities of risky offenders through the review of the records of past convicts and interviews with the victim directly or by observing the scene of crime and the remains of behavior. The perpetrator will provide them with a profile and, as a result, take steps to identify them. What is certain is that this technique does not have the ability to accurately identify perpetrators, but limits the circle of potential suspects so that law enforcement officers can identify the actual perpetrator. It is only possible to use this technique in relation to high-risk crimes and those who are difficult to identify. Hence, this technique can be used to identify some types of cybercriminals. The most common types of semi-circular design are: first; the creation of a view of demographic-social and psychological-behavioral features as well as the motives of former convicts (inductive approach) and Second, studying the scene of crime and then analyzing the data collected from it (deductive approach). In this paper, for the reasons that will be mentioned, the authors focus on the first kind of criminalization in a special sense. According to some criminologists, the findings of this study, which focus on the study of the status of defendants and convicts of cybercrime in Iran, show that criminally liable criminals are not, like all other criminals, formed from a heterogeneous group and their motives are different from criminals. The real world is not. However, some of the features that are presented without scientific-experimental support can be clearly seen in cyber criminals - and not criminals exploiting cyberspace (Tavajohi, 2016).

Today, no sphere of influence and computer intervention is immune, and perhaps it is not unpardonable that in the present world, anyone who has not learned computer skills is a new illiterate. Now, we are talking about how and by what ways such crimes can be prevented, because if committed, they have irreparable consequences for the crime, including the dignity of these individuals and, in many cases, the transfer of their property to In this article, we have tried to propose solutions to prevent and predict the occurrence of such crimes, so that they can be avoided as a result of their persecution and the irreparable consequences that they have, since it appears that those who commit these crimes are those who have full knowledge of the Internet and computer And these crimes can never be mistaken It happens that the computer crime crimes committed by the importation of computers has become widespread in the country since the arrival of computers in the use of the Internet. Internet access to the country began in 1991 and began to evolve in 1993, but during these few years there was no criminal conviction that caused many The computer perpetrators escaped from punishment and continued their crimes, and they also considered the lawfulness of the crime and the charges, which was also cited correctly. By the adoption of the Computer Crimes Act (2009), new concepts and practices were introduced in Iran's criminal law, each of which Requires detailed and expert scrutiny Negro is being debated, you can not ignore the computer (Malmir, 2017).

It should be noted that the abovementioned cyberwarrage and cyberspace research has been discussed in areas such as cybercriminology, differential criminal and criminal policy in the field of computer crime, as well as in the analysis of cybercrime and its challenges and shortcomings. And is discussed in a general and transient way, while the present and future research is seeking a new approach, in the context of analyzing and investigating the computer crime law from crime to guaranteeing execution and victim's rights based on the criminological components of His main mission and his ultimate goal are.

6. Discussion and conclusion

The use of modern communication tools, especially the cyber-environments, has created new opportunities for offenders.

In the same vein, if criminal law within each society fails to adapt to these advances, there are also many crimes and delusions to existence It would seem that it would remain unpunished, perhaps the most important means available to combat new criminal offenses against criminal law. Solutions such as crime, the creation and development of criminal responsibility, the use of modern solutions to disputes and punishments, and, in relation to the criminal liability of criminals in Iran's legislature, has been developing and extending criminal liability against legal persons. . Until the passage of the above law, the criminal jurisdiction of legal persons was not raised in Iran's penal code, and the law on computer crime for the first time accepted this issue of criminal liability of legal persons.

We know that many computer crimes are usually carried out by legal entities, and this Iranian lawmaker's act of criminal responsibility for these individuals is completely normal and is in fact the use of a tool to extend criminal responsibility for combating new crimes, although it must be acknowledged that: The criminal liability of legal persons does not mean the negation of the true responsibility.

Certainly, the criminal policy makers of a criminal system consider the new doctrines in criminal law and criminology in defining the strategy of punishment. Determining this approach depends on the nature of the crime and the characteristics of its perpetrators. Perhaps in the face of crime, the reformist approach can be effective in preventing and combating crime in practice and, in the case of other crimes, make it necessary for a strict criminal policy. Even the new penal system, the New Neoclassical in theory Determine predestination in the realm of special criminals and so-called coarse grains, and accept neglect for minor crimes. Ultimately, if the perpetrator is in a way that is true of him (the effect of zero treatment), that is, a criminal offender of such a crime The category of delinquent is a white collar, and term and treatment are bound to fail. If the rate of this crime and the extent of the victim is such that (in the phenomenon of fear of crime) in society, security is shaken, the resort to the punitive movement must take into consideration the planners in the fight against such crime on the horizons of thought. It should be done.

The development of new technologies and, consequently, the communications and information revolution have led to a huge change in global scenes. Among these new technologies, the Internet has been able to provide a powerful tool in the field of information, which is sometimes referred to as an information explosion. The development of this massive information network has had many benefits for humanity today, although this space and the use of information and communication technology have provided many opportunities for a significant portion of human activities to be carried out at a faster and less costly level, but this information technology facilitates The context of the crime and the development of material and moral damage caused by crime and the creation of new crimes and the creation of new criminal methods have provided many golden opportunities for the perpetrators; in such a space as "cyberspace") It is said that individuals and communities outside the government area play a role The traditional control of governments has faced serious challenges in functional areas such as security, political order, management and organization of economic, social and cultural activities. The challenges that each of them is to insure each government is enough that the scene of these challenges and holes is the names of the perpetrators who have been targeting the security of the people and governments throughout the world.

References

Elham, Gholam Hossein, Borhani, Mohsen, 2013, Income for General Penal Law, Volume I, Tehran, Publishing Mizan, First Printing.

Ansari, Bagher, 2008, Review and Review of the Freedom of Information Bill, Journal of the Legal and Presidential Affairs, No. 13.

Bastani, Boroumand, 2009, Computer and Internet Crime, A New Manifestation of Delinquency, Tehran, Behnamy Publication, Second Edition.

Bakhshi Zadeh, Amin, 2012, Developments in the New Approach to the Islamic Penal Code Bill, Tehran, Cheragh Danesh Publishing, First Edition.

Pakzad, Batul, 2011, Cyber Terrorism; A New Threat Against National Security, First Printing, Tehran, Publishing Office of Science Development Extension.

Tahayori, Farzad, 2004, Unauthorized access to computer systems in Iran's law and international documents, Master's Degree in Criminal Justice and Criminology, Mofid University of Qom.

Jalali Farahani, Amir Hossein, 2006, Cyber Terrorism, Journal of jurisprudence and law, Third year, issue 10.

Jalali, Ali Akbar, 2003, Electronic City, Tehran, Iran University of Science and Technology University Press, First Edition.

Haji Deh Abadi, Ahmad, 2011, Compensation for Victims, Tehran, Publications of the Research Center for Islamic Culture and Thought, Second Edition.

Hasanvi, Reza, Farsaei, Darush, 2002, Computer Literature Culture, Tehran, Associate Press, Second Edition.

Khaleghi Ali, 2013, Criminal Procedure, Tehran, Legal Advice of the City of the 21st Century.

Darbighi, Babak, 2000, Legal, Ethical and Social Challenges in Computer Space, Tehran, Publishing Samat, First Edition.

Dindar, Morteza, 2010, Criminal Liability of Legal Persons in Computer Crimes, Investigative Work 2 Law School, Allameh Tabaabadi.

Rayjan Asli, Mehrdad, 2009, Computer Crime Law: Innovations and Shortcomings, Journal of Legal Research, No. 15.

Rasouli, Meysam, 2011, Cryptographic and Digital Signing Algorithms, Tehran, Pars Book Publishing, First Edition.

Rashidi, Pedram, 2011, Examining Crime Against the Health and Data Integrity in Cyber Space, Master's Degree in Criminal Justice and Criminology, Campus Campus of Qom.

Zargar, Mahmoud, 1382, Principles and Concepts of Information Technology, Tehran, Behinay Publishing, First Printing.

Britton, Dana M. 2011 . the Geder of Crime, New York: Rowman & Littlefield Publishers.

Babchishin, Kelly M. Hanson, R. Karl and Hermann, Chantal A. 2011.

Chiesa, Raoul, Ducci, Stefania and Ciappi, Silvio. 2009 . Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking Boca Raton: Taylor & Francis Group Auerbach Publications.