OPEN ACCESS
Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: http://saudijournals.com/sijlcj/

Original Research Article

Cyber Criminology: Investigating the Characteristics of Internet Crimes and Criminals

Ehsan salami
Master of Criminal Law and Criminology Tehran University Enghelab Square Iran

***Corresponding author:** Ehsan Salimi
| **Received:** 15.03.2019 | **Accepted:** 24.03.2019 | **Published:** 31.03.2019
DOI:10.21276/sijlcj.2019.2.3.2

Abstract

Currently, the Internet is considered as the largest medium and the most important tool for transferring and exchanging information. Besides the benefits and facilities of this "worldwide web", the possibility of crime occurrence has been doubled. Offenses which are now threatening citizens' safety, behavior and welfare, did not exist in the past at all. The present study investigates properties and factors which double the risk and damage of internet crimes. Findings revealed that on one hand internet crimes have unique characteristics such as global aspect, ease of perpetration, extent of damage, multiplicity of victims and crime detection-related issues and the like and on the other hand, internet criminals and victims differ from other criminals and victims in terms of age, gender, motivation and others.

Keywords: Cyber Crimes, Internet Crimes, Crime Characteristics, Criminal Law of Information Technology, Internet Criminal and Victim.

INTRODUCTION

Today, the Internet usage has grown in the human life. It is no exaggeration to say that this great technology has created a new world, a virtual one. Much of daily activities in the life somehow depend on the internet and this dependence is growing increasingly, since the internet, just as the publishing industry, helps the public to create information. It allows data exchange just as the cell phone, facilitates learning and self study just as books and journals, provides entertainment just as the movies and the television, and provides all of these activities simultaneously; however its major property is the ability to interact and provide feedback which makes personalized communications [1]. This great technology that is initiated to provide human beings with more comfort and welfare gradually turned to an instrument for criminals to achieve criminal aspirations as well. In fact, general criminal activities no longer belong to the actual world. Along with the development of cyber activities and communications, some offenders also have shifted their criminal activities into the cyberspace to commit some crimes through such an environment [2]. This new space has brought the traditional criminal law with a fundamental change in which definitions of crimes in virtual spaces do not comply with classic definitions and differ in so many ways [3]. Internet crime is defined as the committable crime on the internet environment whether the internet is a device or a goal [4]. Indeed, cyber crimes refer to violation of law through the use of advanced communication networks such as the Internet, chat rooms, emails, bulletin boards, by a group against other person or group with a criminal impetus to harm victim's reputation and prestige or create physical injury or trauma to the victim directly or indirectly [5]. The scientific study of caused and factors involved in the perpetration of classical crimes via ICT or in the cyberspace, especially the internet, and new crimes against the informatics systems and cyber data, specifically among virtual communities, requires a new criminological approach well suited for this space; accordingly cyberspace criminology as cyber criminal law and procedure is giving birth to its own theorization and principles following actual criminology, in a way that some criminologists professionally study crime and victimization in the virtual world [2].

Characteristics of Internet Crimes

The Ease of Crime Perpetration on the Internet

One of the distinct and valuable characteristics of ICT with respect to other technologies, such as nuclear, biological and Nano-technology, at least at the current juncture is that many individuals with minimal technical skills are able to exploit its various capabilities [6]. Consequently, crime perpetration in the cyberspace is easy as well; every one with a computer, an internet connection and little computer literacy can be a potential offender [7]. For example, someone who

is going to release a fraudulent scheme to deceive people for scams, if looks for victims in the real physical world, certainly will find few targets. Yet in the cyberspace, with minimal cost and technical knowledge he/she can initiate a website and send a deceptive advertising message to users' call numbers or email addresses and attract millions of audience. In addition to the above, what facilitates the perpetration of internet crimes further is that there is no restriction on the cyberspace; for example in committing a bank robbery, planning and designing the robbery, including basic acquaintance with the location, acquiring information of the present status of the bank, financial and security data, and scrutinizing into other details may take a long time. On the other hand, in the actual condition, to avoid being identified by the police and people, all capacities should be held for keeping the perpetrators' measures and identities secret. Still, no such restrictions exist in the cyberspace; hacking into the confidential government systems is easily possible through writing a simple program, without any fear of being identified by others [7]. Moreover, the lack of proximity between the victim and the offender makes such crimes even easier. The presence of the criminal at home rather than at the crime scene will make him/her much more brazened. According to the present statistics, almost 70% of internet users in Iran use the internet in nonpublic places and/or at home [8].

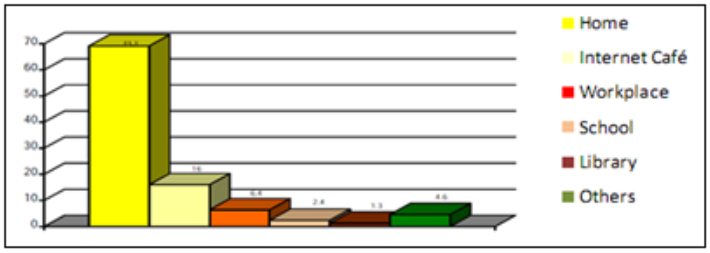

Fig-1

Trans-Boundary Nature

The internet and the cyberspace act independent from the geographical boundaries. They do not limit within the framework of political maps and do not follow any place limitation. The cyber is a borderless expanse which no divider lines can be drawn around it or no natural or artificial borders can separate it or take it apart [7]. In fact trans-boundary data processing has characterized such crimes with the property of internationality [9]. This property allows the presence of potential criminals for every single internet users worldwide, because every one of them may commit a crime in his/her country as that in other countries. For example, the following event best elucidates the trans-boundary aspect of the cyber:

A threatening email containing a bombing threat was received in a grocery store in Latvia. Frequent investigation revealed that the perpetrator is living in Estonia who actualized his measures via the cyberspace. In another case an anonymous person threatened the Norwegian headquarter of the police staff with bombing. Consequent pursuit did not identify the perpetrator. With the help of Norway Interpol, the Canadian government found that the perpetrator had registered a domain in the country and uses Canadian lines. Although Interpol expected the person to live in Canada, plenty of investigations revealed that the perpetrator resides in the neighborhood of the Norwegian police headquarter [10].

The Extent of Damage Due to Crime

The damage of the Internet crimes is far greater than that of traditional crimes. Interestingly, the cost and the inconvenience of the extensive amount of damage are far lower for internet victims than those for traditional victims; in other words, a computer criminal enters the internet networks with the minimum facilities and imposes maximum damage to the government and other users. For example, according to estimations by experts, the damage to computer systems by the spread of the virus "I love you" has been over 11 billion dollars, which is unique regarding the extent of losses [7]. Another instance is the virus that caused tens of thousands of PC's not to start up on March 6, 1992. The virus named Michelangelo and is programmed to be activated on Michelangelo's date of birth. The Michelangelo virus was first detected on April 1991. Some of the users who had received the warnings did not start up their PC's on March 6 to be safe from its aftermath. However, many computers at large organizations including the New York subway were infected by the virus. The virus caused losses in the UK, Japan and South Africa as well [11].

Issues of Crime Detection and Criminal Prosecution

One of the challenges of the Internet crimes is the issue of detection. In such crimes, due to their occurrence in virtual and unreal space, no tangible and physical sign of the crime and criminal's trace, as left in traditional crimes, are observed. In many cases, those very left traces of the crime which are traceable are simply removable. Therefore, it could be argued that likely the black figure of the Internet crimes is higher than that of traditional crimes [12]. High black figure in the Internet crimes is due to several reasons, including difficulty of crime detection, crime complexity and companies and banks' unwillingness to disclose these crimes for their fear of losing customers and their trust.

However, no secure and proven method has been found to detect and prosecute these crimes. Formal problems in the stage of detection and prosecution of cyber crimes are not limited here; in many cases even

after the detection, the offender is miles away from law enforcers and juridical authorities and he/she cannot be prosecuted. Yet, the level of international collaborations is not appropriate to create strong and coordinated strategies to combat such crimes. Even there is no international act that characterizes such crimes as a global issue in a way that the criminal receives investigations and punishments based on international regularities [7].

The Absence of Control and Monitoring on the Cyberspace

Nowadays, the Internet is interpreted, at least theoretically, as a lawless, unrestricted, unregulated, uncontrolled, and accessible environment [13]. The cyberspace is a space which has no specific international institution or organization to govern and control, this is while controlling and monitoring this space is very cumbersome and perhaps impossible; since the network and cyberspace is a lateral environment rather than a linear one and every individuals, who have communicate with each other across the world, have the same amount of rights in this virtual space.

For example, today, social networking is one of the most salient manifestations of a lateral environment with no hierarchy of members. Individuals who experience virtual communities have different understanding of such communities based on their needs and conditions. Some definitions emphasize on the pleasure and desirability of these communities, while other definitions strongly emphasize the information exchange in this kind of communities [12]. Generally, virtual communities can be defined as a group of people that communicate through electronic media, such as the internet, and share their interest, geographical locations, physical interactions or national origins without enduring pressures derived from formation real-life communities [14, 15].

Moreover, monitoring these communications not only in many cases conflicts with individuals' rights and privacy, but also practically seems impossible. This environment has no dominant police. In the declaration of independence of the cyberspace, it has been honored and it is stated:"Hey, governments of the industrial world! Hey, dull giants made of metal and sensuality! I am the resident cyber….Where we come together, you have no sovereignty….We have no elected government and hope there be no government here" [16]. It could be argued that as much as the cyber environment is leading technologically and technically, it has not developed monitoring structures and sufficiency/abilities. This may be the result of its high technical speed of development which causes the monitoring to hinder behind in a way that some claims that the cyberspace is a technological cold and exanimate space in which what is so-called as group consciousness, social guiding norm, cooperate ethics etc. and founds the basic of order in every society, are meaningless. In every society and/or environment, even animal environments, some social controllers hierarchically monitor individuals' behavior and functions within the framework of inferiors' obedience of superiors. However the cyberspace is an open environment and free from any type of social norms and pyramidal hierarchies of monitoring and obedience [7]. Apparently, this perspective toward the cyberspace is not exempt from problems. Although the cyberspace has no specific and dominant monitoring organization and/or institution, in some cases computer and the Internet users have to observe undefined norms which can be interpreted as cyber unwritten law/conventions, though pallid, and where they're not respected, website managers or other users will deprived the corresponding user/s of exploiting the facilities on the related virtual space. For example, observing the propriety in chat rooms is one of the cases which if not obeyed, other members will exclude the violator from being in the room.

High-Speed Development of Computer Technology

Extremely rapid development of the computer technology has made modern methods of crime unknown and anonymous, causing the legislators not to be able to criminalize. For example, the traditional robbery is perpetrated through many ways such as pick-pocketing, bank holdup, lift and etc. According to these methods, the legislator has initiated to criminalize different types of robbery in the Islamic criminal law. Yet, in computer crimes, in addition to different ways for perpetrating a crime, sometimes new and unknown crimes can come across such that even appreciation of their conceptual meanings is hard for jurists and judges. This stems in the high-speed development of technology and ICT. It may be argued that due to this swift development, the penal legislator is always a step behind the technology and initiates criminalization after victimization of many citizens by smart computer criminals.

Characteristics of the Internet Criminal and Victim

Age of Criminals and Gender of Victims

Age of Criminals and Victims

The extent of using the Internet and virtual networks is so increasing that the current generation is called the generation Z of the Internet or network generation. This generation consists of those who were born in the middle of 1990s onward. There exist considerable differences between generations' use of social networking and also their motivations for joining the virtual space [17]. Adolescence is one of the age groups who represent strong interest in the Internet. This medium has a special position among teenagers all over the world via its multiplicity and also the power of attraction. Based on the recent studies conducted at the research institute Pio on the effect of the Internet on adolescents' lives, about 93% of American adolescents use the Internet and mostly share contents such as video files, pictures, and school and nonschool texts, 28% of

them run weblogs and prefer the Internet to the television and the movies. Accordingly, boys like to share videos and girls are interested in blogging and sharing pictures. The results of the study are summarized in the following table [18].

Another characteristics of the Internet crimes which is a serious warning for the modern societies, is the exposure to a large group of adolescent offenders, some of whom are not reached the legal age. However, their alleged crimes on the Internet have much more extensive losses that those in the traditional crimes. For instance, a 15 years old adolescent who had an 89000 dollars phone bill on the account of some companies was detected and arrested. This offender used a modem and a PC at home to hack computer systems at commercial firms. Through the application of this plan, he obtained their password, thereby he could call from everywhere on the account of the company (Computer Report Monthly). In another cases, "Telenet" and "Datapack" computer networks can be exemplified. Users of these two networks, within a week, set complaints to the administrators and protested that someone hacked their systems and caused serious problems. Since the electronic abuse had a transnational status, Canadian police along with US police arrested four 13 years old teenagers at Dalton school in New York via electronic lines of the networks [19]. The following diagram clearly depicts that young individuals, aged 16 to 24, and had the highest Internet use in the countries under study [20].

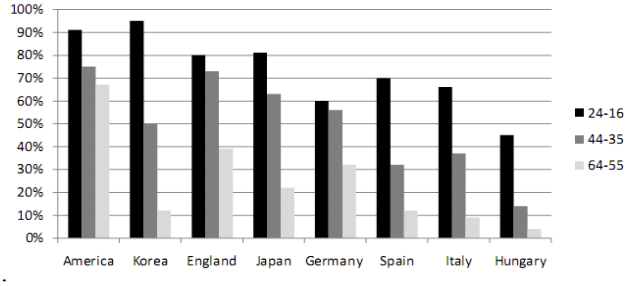

Fig-2: the use of Internet based on age 2003
Extracted from http://www.worldinternetproject.net

Gender of Victims

Today, individuals' access to the Internet and knowledge of cultural manifestations around the world occur easily. Adolescents, who are more impressionable and curious than other people, are much more exposed to the aftermaths of such manifestations. Here, the difference of information selection in boys' and girls' use of these consignments and also their impressionability should be considered and investigated. Girls incline to attract attentions, establish love, friendship and fashion, while boys intend to be entertained and shop on the Internet [13]. Generally, boys use more emailing, purchase, information searching and pornography than girls, whereas girls who prefer to establish emotional relationships since they do not trust the Internet fully [21].

Gender may increase the probability of victimization [22]. However, the authors of EU convention and jurists from different countries have never considered the victimization of women in the cyberspace in line with other crimes such as pornography against children or hack. Therefore, victimized women have remained as secondary concerns for all societies with virtual systems. This drop-out is clearly observable within the growth of rate of criminal events which target women in social networking [9]. Among the cyber crimes, there appear special crimes in which the victims are mostly women and children [[1]]. These crimes fall within the domain of what is today referred as the sex industry. The sex industry exploits offensive contents of pornography against women and children and credits for the formerly used dirty pornographies [8]. The most disturbing matter about such data is that not only the sex industry is considered as a big industry, but also the sale of products, pornography, prostitution, and sex tourism are mostly related to women and children (Ibid, 285). In this regard, article 14 of the UN's guidelines for prevention of crime claims: "approaches to crime prevention should consider, if necessary, the differences between man and woman's needs and pay special attention to specific needs of the vulnerable class" [23]. The main reason why online victimization of women in the social networking is increasing is due to the lack of appropriate public cyber laws which are gender-sensitive [9]. Most of the Internet users in Iran are men as well. Moreover, almost all of the cyber crimes are perpetrated by men. Accordingly, women are more exposed to victimization. The disturbing issue is that 95% of computer criminals in Iran are men; the majority of them are in the 18-35 age groups [[2]], 8]. The following chart depicts that 70% of users are men and 30% are women.

[1] Stalking, morphing, cyber sex, Issues of cyber privacy and Pornography

[2] Cited in ICT news, Omidi, Mehrdad (deputy for combating special computer crimes) at http://www.cra.ir

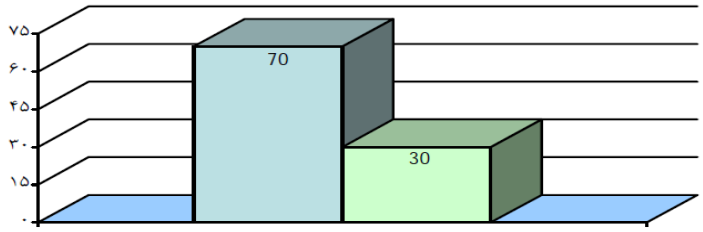

Fig-3

Lack of Remorse after Crime Perpetration

Another issue which doubles the risk of cyber crimes with respect to traditional ones is the absence of sense of remorse and the lack of feeling guilty on the side of criminals, which is the salient feature of the majority of sophisticated crimes. A significant number of the Internet users only use the Internet to spend time [8]. The following diagram depicts users' tendencies on the internet.

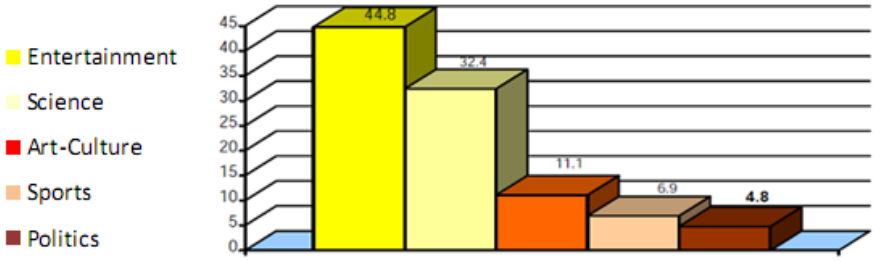

Fig-4: Concerns of young people on the Internet

In such crimes, not only does the offender feel remorse, but also conversely prides on his/her intelligence and ability to perpetrate these offensive activities and somehow feels bright. Although there is no precise statistics, it seems that in cyber crimes, the crime is numerous and repetitively perpetrated which is partly due to offenders' lack of remorse and conscience.

Multiplicity of Victims

In the Internet crimes, usually there is no precise statistics of the number of victims; since firstly, complaints of the Internet criminals is not so usual and common and cyberspace users seek to enhance the security equipments of the system and disposal of the crime rather than criminal prosecution. Antivirus programs are among this type of combat. Secondly, considering the network communications in the cyberspace and the virtual world, many victims contribute to spread the crime mistakenly and in some cases automatically. For example, when a virus spreads, the victim him/herself causes losses and damage to other, though wrongly. The issue of victim's involvement in the spread of viruses exponentially increases the number of victims. Another factor which has the same consequences is the public nature of the Internet and its high number of users. In other words, the Internet is a public media which has many users and audiences in different parts of the world. Considering the high number of users on the Internet, a crime, though with a traditional nature such as insult, will entail many victims.

CONCLUSION

Along with the functions and abilities of the Internet to aid people with much more welfare, perpetration of traditional crimes such as theft and fraud have been facilitated and yet more dangerous. Internet crimes differ from traditional crimes in crime typology, criminal and victim. In fact, perpetration of such crimes is far easier. These crimes have global and trans-boundary aspects: detection, prosecution. Therefore, arresting related criminals is far more difficult than other crimes and the extent of damage and losses by these crimes are incomparable with other types of offenses. The high speed of growth of the Internet complicates the process of monitoring and control. These crimes differ from other offenses in terms of victim's and criminal's situation as well. Here, the criminal is more intelligent and younger, with no sense of remorse and regret after the perpetration. Additionally, the number of victims in such crimes is much higher that traditional crimes. Most of the Internet victims are women. Due to such characteristics and other properties, mentioned in the present study, the doubled risk of the Internet crimes with respect to other crimes is obvious. The extent and severity of the damage and losses and the increasing number of these crimes demand more serious consideration by the legal community; since it could be certainly stated that in future we are exposed to higher numbers of such crimes

and if the society, media and law are indifferent toward these offenses, they would not be combated correctly and seriously whether at the levels of prevention, legislation or punishment. Finally, it should be stated that the Internet and the space of information exchange, play an inevitable role in our personal and social life. In spite of all challenges and dangers of this communication device, its advantages and functions cannot be overlooked. In other words, modern communication technologies have several advantages and disadvantages. Therefore, considering the social power of this technology, ICT which is striving toward the development and change in social communications, should be further investigated [10]. Thus, policy makers in Iran should be more concerned with various dimensions of this technology. On the one hand, they should provide necessary infrastructures to prevent internet crimes and on the other hand create the appropriate facilities/possibilities to maximize exploitation of the Internet.

REFERENCES

1. Selnow, Gary. (2000).The Internet: The Soil of Democracy, Vital speeches of the Day, New York, nov: 1.
2. Pika, G. (2011). Criminology. Translated by: Najafi Abrand Abadi, A.H. 2nd Edition. Mizan Press.
3. Hassan, Beigi, E. (2005). Rights and Security in Cyberspace. Tehran: Contemporary Abrar International Research Institute.
4. A'lipour, H. (2011). Criminal Law of Information Technology. 1st Edition. Tehran: Pleasure Publication.
5. Halder, D., & Jaishankar, K. (2011). Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA, IGI Global.
6. Jalali Farahani, A.H. (2010). An Introduction to Procedures of Criminal Litigation of Cyber Crimes. Tehran: Khorsandi Publication, 1st Edition.
7. Fazli, M. (2010). Criminal Responsibility in Cyberspace. 1st Edition. Pleasure Publication.
8. Hajili, M. (2009). The Situation of Communication Technology of Youth. The Supreme Council of Information.
9. Jaishankar, k. (2011). *Cyber Criminology, Exploring Internet Crimesand Criminal Behavior*, Boca Raton, CRC Press.
10. Shirzad, K. (2009). Computer Crime from the Perspective of Iran Criminal and International Law. 1st Edition. Tehran: Optimum Publication.
11. Nagpal, R. (2008). *Cyber Crime and Corporate Liability*. Wolters Kluwer India.
12. Lee, H.Y. Ahn, H. Han, I.(2006) Analysis of trust in the E-commerce adoption, Proceedings of the 39th Hawaii International Conference on System Sciences.
13. Kornblum, Janet. (2007). "Indersexes", us today :www.ustoday.com
14. Barnatt, C. (1998). Virtual communities and financial services-on-line business potentials and strategic choice. *International Journal of Bank Marketing*, *16*(4), 161-169.
15. Romm, C., Pliskin, N., & Clarke, R. (1997). Virtual communities and society: Toward an integrative three phase model. *International journal of information management*, *17*(4), 261-270.
16. BARLOW'S, J. P. (1996). Declaration ofindependence for cyberspace.
17. Bartholomew, M. K., Schoppe- Sullivan, S. J., Glassman, M., Kamp Dush, C. M., & Sullivan, J. M. (2012). New parents' Facebook use at the transition to parenthood. *Family relations*. *61*(3), 455-469.
18. Peattie, S. (2002). Using the internet to communicate the sun-safety message to teenagers. *Health education*. *102*(5), 210-218.
19. Pakzad, B. (1996). Computer Crimes. MSc Thesis, Shahid Beheshti University.
20. Tavakol, M., Kazempour, E. (2005). Social Transformation in an Information Society. Tehran: The National Commission of UNESCO Press.
21. Taci, C. Line. (2001), "Developing an Interment attitude scale for high school student" Black Coach press, London.
22. Najabati, M. (2000). The Role of Proper Design of Residential Units in the Prevention of Crime. Journal of Security. 4(16).
23. Javan, Ja'fari, A.R. and Seyyedzade Sani, M. (2012). Practical Guidelines for prevention of Crime. Deputy of Prevention of Crime of the Judiciary. Tehran: Mizan Publication.