Cyber-Crimes in Iran: Definition and Analysis

Fatemeh Sajedi 1
Department of Law, Research and Science Branch, IAU, Sistan and Balouchestan, Iran
Email: fathimasajedi@gmail.com
Mohsen Ghasemi Ariani 2
Department of English, Research and Science Branch, IAU, Neyshabur, Iran
Email: mohsenghsemiariani@yahoo.com

ABSTRACT

The cyber-crime as a notorious phenomenon threats nation's security and financial health. And due to the development of internet technology, computer systems offer some opportunities for law breakings in Iran. Besides, Iranian policy makers are trying to prevent sabotage activities through the internet. While new cyber-related cases are increasing, Iranian Cyber Police (FATA) tries to discover and detect them. The present study is aimed at defining and classifying cyber-crime, its nature, and advantages and risks. It also directed it attention to scrutinize Iranian teachers' attitudes towards this classification and what happens in reality. Based on interviews with university teachers, analyses show that some elements such as costs of cyber-crime, weaknesses of the current system, role of Iranian cyber police (FATA), and cyber security are fundamental factors. More importantly, the finding demonstrated that FATA should improve its infrastructures more to reinforce it abilities, hold more workshops and national conferences and also other Iranian official organizations such as Iran National Media and Legal System have to take serious actions.

KEYWORDS

Cyber-crime, Classification, and Iranian Teachers' Attitudes

1 INTRODUCTION

Cyber criminals increasingly invade the information structures misusing new technology and these attacks not only impose expensive costs on society but also are increasing at alarming rates. Unfortunately, cyber wrongdoers impair public trust and endanger substantial reliance of people upon transactions and information infrastructure. Consequently, up-to-date information necessary to face cyber-attacks is urgent [1]. Besides, cyber-crime is a substantial phenomenon that still requires to be fully understood [2], [3]. Cyberspace as a social space includes information and communication infrastructures that underline internetworked systems. Although the amount of cyber-crime is increasing, cybersecurity is a case that should be paid attention carefully. Cyber-crimes such as computer abuses, cyber-trespass and malicious software that are new forms of crime are more advanced ways than traditional crimes including blackmailing, fraud and hidden communications. Traditional crimes and cybercrimes as ominous phenomena have been committed and sued for years [2], [3]. These crimes aim the financial and transactional security of people and nations. The present study directs its attention to cyber-crime and its footing in Iran. More importantly, the challenge of controlling cyber-crime requires a full range of steps which should be taken. Because technology systems are vulnerable, Iranian government should develop and enhance their crisis management processes to enable cyber spaces to continue operating.

2 NATURE of CYBER-CRIME

Cyber-crime, returning to the definition provided by Casey, refers to any crime that

involves a computer and network, where a computer may or may not have played an instrumental part in the commission of the crime. The term cyber-crime would be used to refer to a criminal act like that of identity theft, which involves the theft of someone's personal information such as their credit card number or Social Security number [4].

3 ADVANTAGES and RISKS

The introduction of information and communication technologies (ICTs) into many aspects of everyday life has led to the development of the modern concept of the information society. This development of the information society offers great opportunities. Although unhindered access to information can cover democracy, uncontrolled and free access paves the way for cyber wrongdoers. The growth of technology and information are accompanied by serious threats that sometimes have its side effects. They threaten finance and communication infrastructure and also endanger the smooth functioning of information technologies. Unfortunately, cyber-attacks are difficult to foresee and internet services are vulnerable and have the potential to harm society and wrongdoers take advantage of the vulnerability [5]. So, we should take serious actions to safe information and communication infrastructures.

4 CLASSIFICATION of CYBER-CRIME

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. 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 [6].

5 IRANIAN TEACHERS' ATTITUDES

The beliefs of ten native PHD law teachers of Azad University of Mashhad toward cyber-crimes and their impacts on Iranian society had been studied. Teachers were chosen as a case. Choosing a case is not necessarily concerned with representativeness and typicality of the case but with its accessibility and the opportunity it provides to the researcher to learn [7]. To this end, they were interviewed separately to express their opinions, experiences and priorities about the main important committed elements of cyber-crimes in Iran. In fact, the interviews were conducted in person at Azad University and the data was recorded. Based on interview with the teachers, the findings reveal that paying serious attention to some elements such as costs of cyber-crime, weaknesses of the current system, role of Iranian cyber police (FATA), cyber security and cyber-crime is urgent. .

6 COSTS of CYBER-CRIME

Cyber-crimes continue to be costly and have become common occurrences in Iran. Although the cost of cyber-crime varies by individual and organizational size, it is difficult to measure and the estimated annual cost over cyber-crime is not clear. But what is clear is that cyber-crimes

imposed expensive expenses on persons and organizations, and judiciary service which it takes a lot of time and money to sue the cases in Iran and it may lead to discouragement has to invest and cooperate with academic professionals. Because of huge costs of cyber-crime, a comprehensive national investigation is necessary for all aspects of this ominous phenomenon by Iranian policy makers. The investigation should involve a review of the initial complaints, inspection of the alleged damages or imposed costs, examination of the system logs and, finally, strong actions.

7 WEAKNESSES of the CURRNET SYSTEM

The open and defiant manner in which hackers currently operate reflects the weakness of the legal, defensive, and investigative capacities of the current system [1].Though law enforcement personnel were able to anticipate some types of cyber-attacks, they were not able to prevent it. So, law enforcement agencies with the aid of professionals should spend countless hours fighting cyber-crime each day to prevent this dangerous phenomenon. Prevention is always better than cure. 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 different kinds of crimes and criminals more possible [5].

8 ROLES of IRANIAN CYBER POLICE (FATA)

The Iranian Cyber Police (FATA) is a unit of the Islamic Republic of Iran Police, founded in January 2011 to secure cyber space. The cyber police issues new guidelines for individuals and organizations requiring users to provide personal information and it tries to detect and sue the criminal acts related to cyberspace. The growth and influence of the Internet and technology indicate the rapidly growing inclination towards cyberspace, but information technology entails both threats and opportunities. To this end, Cyber Police concentrates on the technical aspects of cyber-crime such as the technical implementations that can be used to deter cyber-crime, the manner in which cyber-crime should be investigated. Apparently, Fata is the only active organization that plays the main role. The objectives of cyber police consist of protection of national and religious identity, community values, legal liberty and preservation of Interests, national authority in cyberspace, protection of national critical infrastructure against electronic attacks, assuring people in all legal affairs such as economic, social and cultural activities in order to preserve national power and sovereignty.

9 CYBER SECURITY and CYBER-CRIME

Cyber-crime and cyber security are issues that can hardly be separated in an interconnected environment. Cyber-crime as a big challenge impairs information and communication systems and serious actions should be taken to secure cyber spaces. Cybersecurity can act as a defensive nature to safe information technology and internet services. Economic welfare and its security are essential to societies and they try to protect their infrastructures and inform technology users. Distinguishing and discovering cyber-crime as a major component of the cybersecurity plays a main role. As well, prevention is better than cure. This requires the adoption of appropriate programs and activities to enhance critical infrastructures and information technologies. At the national level, policy makers should take coordinated actions and pave the way for professionals and executive officials to prevent and safe information infrastructures. At the international level, nations can cooperate with each other to promote the security of communication and

information technologies [6]. Due to the promotion of cybersecurity, making the cyber safer and protecting the user require the correlations of nations and governments. To this end, Cyber Police (Fata) as the only center tries to cope with cyber-crimes, but it needs more help to inform people and Mass media can play an important role in this way.

10 CONCLUSION

Cyber-crime is essentially committed on or with the help of cyber technology. Therefore, scope of cyber-crimes and it footing should be paid attention carefully. The present study directs it attention to the overview of some aspects of cyber-crimes and it also demonstrates that cyber security is urgent. Due to side effects of cybercrimes, the legal and scientific instruments should be used to prevent cyber-crime and promote cybersecurity in Iran. Besides, Iranian Law-enforcement agencies can use the increasing power of information technology and complex forensic software to speed up investigations and automate search procedures. On the other hand, procedures developed to trace out the traditional crimes may not be useful in case of cyber-crime. Therefore, Judiciary service should pay serious attention to cyber-crimes with the aim of science, technology and professionals. As well, FATA can enhance its scientific and technical infrastructure and should formulate new strategies to prevent such attacks and develop countermeasures. With the growing number of people who watch TV and listen to the radio, Iran National Media have to play an important role to inform its interlocutors.

REFERENCES

[1] A. D. Soafer and S.E. Goodman, Cyber-crime and Security: The transnational Dimension. California: Hoover, 2010.

[2] D. Wall, Cybercrime. Cambridge: Polity Press, 2007.

[3] S.W. Brenner, Cybercrime: Criminal Thereat from Cyberspace. Santa Barbara: Praeger, 2010.

[4] R. Moore, Cyber-crime: Investigating high-technology Computer Crime. Cleveland: Anderson, 2005.

[5] M. Malmir, Organized Cyber-Crimes: An Approach on Islamic and Iranian Legal Systems. Journal of Basic and Applied Scientific Research. 3(3) 952-957, 2013

[6] M. Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal response. Geneva: ITU publication, 2012.

[7] R.E. Stake, 'Case studies' in N. K. Denzin and Y. S. Lincoln (eds.).Handbook of Qualitative Research (second edition). Thousand Oaks: Sage Publications, 2000.