Humanities and Social Sciences
2014; 2(2): 33-37
Published online March 20, 2014 (http://www.sciencepublishinggroup.com/j/hss)
doi: 10.11648/j.hss.20140202.14

A global perspective on cybercrime

Kobra Mamandi[1, *], Saeideh Yari[2]

[1]M. A. Law Criminal and Criminology, Qom Branch, Islamic Azad University, Qom, Iran
[2]M. A. Law Criminal and Criminology, Science and Research Branch, Islamic Azad University, Qom, Iran

Email address:
Kobra_Mamandi@yahoo.com (K. Mamandi), Saeideh_yari@yahoo.com (S. Yari)

To cite this article:
Kobra Mamandi, Saeideh Yari. A Global Perspective on Cybercrime. *Humanities and Social Sciences.* Vol. 2, No. 2, 2014, pp. 33-37.
doi: 10.11648/j.hss.20140202.14

Abstract: Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Society is becoming more dependent upon data and networks to operate our businesses, government, national defense and other critical functions. Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace". Thus, it is necessary to introduce cybercrime detailed. This paper gives detailed information regarding cybercrime, its types, and modes of cybercrime. Cyber Crime from the world but we can reduce it to a large extent by creating awareness in Society. We suggest a system of administrative regulation backed by criminal sanctions that will provide the incentives necessary to create a workable deterrent to cybercrime. This new model is compared to some important existing models and applied to cybercrime. This paper is aimed particularly at readers concerned with major systems employed in medium to large commercial or industrial enterprises.

Keywords: Cybercrime, Cyberspace, Hacking, Crime, Computer

1. Introduction

The history of crime and crime prevention has been akin to the history of warfare: an offense is developed, then a defense counters the offense, then a new offense counters the new defense. Machine guns led to the development of tanks which led to the development of rocket propelled grenades, etc. Cybercrimes are everywhere, can happen to anyone, in any time. Some examples of cybercrime are identifying theft, storing illegal information, computer viruses, and fraud. We will discuss about each example in detail. Cybercrime is a new type of crime that occurs in this Science and Technology years. There are a lot of definitions for cybercrime. According to Wikipidia.com cybercrime also known as computer crime that refers to any crime that involves a computer and a network. Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Besides that cybercrime can be defined as crimes committed on the internet using the computer as either a tool or a targeted victim (Joseph A E, 2006). Computer can be considers as a tool in cybercrime when the individual is the main target of cybercrime. But computer can be considers as target when the crime is directed to the computer. In addition, cybercrime also includes traditional crimes that been conducted with the access of Internet. For example hate crimes, telemarketing Internet fraud, identity theft, and credit card account thefts. In simple word, cybercrime can be defined as any violence action that been conducted by using computer or other devices with the access of internet. This action can give harmful effects to other. There are two major categories of cybercrimes which are crimes against the person, property and the government. The first category of cybercrimes is Cybercrimes against governments constitute another level of crime. The second category is cybercrime can take the contents of individual bank account. One widespread method of getting people's bank account details is the money transfer email scam. People receive emails requesting help with transferring funds from another country. Hacking into company websites is property trespass, and stealing information is property theft. Internet time theft also one of the cybercrime against property. It is done by an authorized person in the usage of the internet hours which is actually paid by another person. Cyber terrorism is the most serious type of crime in this category. Hacking into a government website, particularly the military sites, is one manifestation of cyber terrorism. The example of cybercrime against government is web jacking. By web jacking, hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

2. Description of the Cybercrime

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. “The range of technology-enabled crime is always evolving; both as a function of technological change and in terms of social interaction with new technologies” [1].

There are almost as many terms to describe cybercrime as there are cybercrimes. Early descriptions included ‘computer crime’, ‘computer related crime’ or ‘crime by computer’ [2]. “As digital technology became more pervasive, terms such as ‘high-technology’ or ‘information-age’ crime were added to the lexicon” [3]. The advent of the Internet brought us ‘cybercrime’ and ‘Internet’ or ‘net’ crime [4]. Other variants include ‘digital’, ‘electronic’ (or ‘e-’), ‘virtual’, ‘IT’, ‘high-tech’ and ‘technology enabled’ crime. Cybercrime is only important to a few people, but it should be important to everyone. If everyone becomes aware of the dangers of being online, the dangers will slowly disappear. It only if anybody tries to understand the potential harm the Cybercrime may cause can understand the danger of Cyber criminality. Computers, despite being such high technology devices, are extremely vulnerable. The description is not imaginary that to steal the national secrets from any government office or any information about military equipment’s from the computers of respective organization is comparative more easily than to steal a loaf of bread from stall of unattained hawkers standing side by road. All over again, the risk involve the committing Cybercrime is very less due to its special characteristics.

3. The Challenges of Cybercrime and Cyberspace

Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and Hackers has grown into a mature and sophisticated threat to the open nature of the internet. Cyber-criminals, like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced web sites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security [5]. Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities. The Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few. Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve. At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. As a result of rapid adoption of Cybercrime may be defined in a narrow sense as any offence targeting computer data and systems or in a very broad sense as any offence involving a computer system. The first one risks being too restrictive as it would exclude phenomena that do exist in the physical world but have gained a different quality and impact through the use of computers, such as child pornography, fraud or intellectual property right violations. The latter would be too broad as most crime nowadays involves a computer in one way or the other. It is therefore expedient to apply a definition that covers new types of crime as well as old types of crime using computers without being too broad and therefore meaningless. The definition should be sufficiently robust to cover all relevant types of conduct even if technology evolves and phenomena of cybercrime appear to change almost every day. Finally, it should be possible to operationalize it for criminal law purposes in order to meet the rule of law principle that there cannot be a crime without a law. Only conduct established as a criminal offence can be considered a crime. It has been said that there are three factors necessary for the commission of crime: a supply of motivated offenders, the availability of suitable opportunities and the absence of capable guardians [6]. On all three counts, the digital environment provides fertile ground for offending. While specific impacts will be discussed in subsequent chapters, it is useful to summarize briefly some of the key features of digital technology which facilitate crime and hamper law enforcement. Unlike more traditional forms of communication, the Internet allows users to communicate with many people, cheaply and easily “The estimated 1.6 billion people on the Internet, approximately 24 per cent of the world’s population provide an unprecedented pool of potential offenders and victims” [7]. This acts as a ‘force multiplier’, allowing offending to be committed on a scale that could not be achieved in the offline environment [8]. The ability to automate certain processes further amplifies this effect. Not so long ago, computers were large, cumbersome devices utilized primarily by government, research and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims. One problem with Cybercrime is its complexity to understand and safeguards. No doubt, computers are boon and it is very good servant as well having lot of potentiality. It works fast, effectively, efficiently, accurately, without taking pause, and continuously. But after all computers works through programs specially design for the purpose. Cyberspace is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act.

The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber Space Security Management has already become an important component of National Security Management, Military related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in cyberspace. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat. It is, therefore, necessary to put in place a 'National Cyber Space Security Management Policy' to define the tasks, specify responsibilities of individual agencies with an integrated architecture. These programs are written in several lines compatible to computer readable language. These programs have some tips, instructions, processes and logic to be followed by operating systems. Operating systems are composed of millions of lines of code and no single individual can claim to understand the security imply ions of every bit of these computer instructions. The hackers are always in search of any lacuna or loopholes of this programming system.

4. Hacking

The term “hacking” is used to describe the unlawful access of a computer system. It is one of the oldest computer-related crimes, and in recent years has become a mass phenomenon. By targeting computer systems that host large databases, offenders can obtain identity-related data on a large scale, and this is an increasingly popular approach. In the largest case detected in the past in the USA, the thieves obtained more than 40,000,000 credit card records. Apart from direct financial profit, offenders can use identity-related information for other purposes, including using a victim’s bank account to launder money. In addition, they can circumvent identification and terrorist prevention measures by using obtained identities. The Report of the Secretary- General of the United Nations on Recommendations for a global counter-terrorism strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism. Thus, Hackers infringe the laws for a number of reasons such in the order from less harmful to more serious (if we can even classify them this way). Hackers do it:

1. Because they know how and can, either being smart and figuring out how to, or getting the instructions and tools from friends-hackers.
2. Because they get a trill of doing illegal activities and hoping not to get caught.
3. Because they seek publicity.
4. Because they want to take a revenge

5. Differentiating Cybercrime from other Crime

In May 2007 the European Commission issued a Communication towards a general policy on the fight against cybercrime", noting that there was not even an agreed definition of cybercrime [9]. It proposed a threefold definition: 1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems; 2. the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred); 3. A crime unique to electronic networks e.g., attacks against information systems, denial of service and hacking.

6. Development of Computer Crime and Cybercrime

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed. In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology. At this early stage, offences focused on physical damage to computer systems and stored data. Such incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university. In the mid-1960s, the United States started a debate on the creation of a central data-storage authority for all ministries. Within this context, possible criminal abuse of databases and the related risks to privacy were discussed. In the 1970s, the use of computer systems and computer data increased further.

At the end of the decade, an estimated number of 100000 mainframe computers were operating in the United States.With falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems121 that had dominated the 1960s, to new forms of crime. While physical damage continued to be a relevant form of criminal abuse against computer systems, new forms of computer crime were recognized. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer-operated transactions led to another new form of crime computer-related fraud. Already at this time, multimillion dollar losses were caused by Computer-related fraud. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cybercrime. Interpol discussed the phenomena and possibilities for legal response. In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. The interconnection of computer systems brought about new types of offence. Networks enabled offenders to enter a computer system without being present at the crime scene. In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the process. OECD and the Council of Europe set up study groups to analyses the phenomena and evaluate possibilities for legal response. The introduction of the graphical interface in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally even in countries where the publication of such information was criminalized.

Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990 and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples as in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as phishing, and botnet attacks, and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as voice-over-IP communication and cloud computing. It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

7. Conclusion

As suggested earlier in this paper individual interest for use of available technology, national interest to secure its community from inner and outer threat, sovereign privilege of noninterference of any extra-territorial authority, trade and developmental thrusts are major consideration in the area of Cyberspace. However, it is sure, that evolution is irreversible process and we cannot step back from it. What remain in our hand is to change the direction of progress, and we stick up to our commitment to turn it in the direction of sustainable development. Thus, we all agree that more businesses are converting their data to format. Hacking as part of cybercrime is definitely moving forward, with new tools to hack and new viruses to spread coming out every day. The urgent need of information security, ethical education and awareness programs cannot be emphasize enough in order to achieve the maximum protection from the hackers and also to protect Cyber world from our own abusive use.

References

[1] G. Urbas and K. R. Choo, ResourceMaterials on Technology-Enabled Crime, Technical and Background Paper no. 28 (AIC, 2008), p.5.

[2] House of Commons Standing Committee On Justice And Legal Affairs, Computer Crime, Final Report (1983), p. 12; Sieber, Legal Aspects of Computer-Related Crime and Parker, Crime by Computer.

[3] S. W. Brenner, ‘Cybercrime metrics: Old wine, new bottles?’ (2004) 9 Virginia Journal of Law and Technology 1, n. 4.

[4] Morris, The Future of Netcrime, p. vi.

[5] Michael Hatcher et al., Computer Crimes, 36 AM. CRIM. L. REV. 397, 399 (1999).

[6] L. Cohen and M. Felson, ‘Social change and crime rate trends: Aroutine activity approach’ (1979) 44 American Sociological Review 588, 589.

[7] Internet World Stats, Internet Usage Statistics: The Internet big picture – world Internet users and population stats (2009), www.internetworldstats.com/stats.htm.

[8] Model Criminal Code Officers Committee of the Standing Committee of Attorneys- General, Chapter 4: Damage and Computer Offences, Final Report (2001), p. 95.

[9] European Commission. Towards a general policy on the fight against cybercrime, May 2007. COM(2007) 267 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.