ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Taxonomy of Cyber Crimes and Legislation in Saudi Arabia

Naasir Kamaal Khan

ABSTRACT **- Recent developments in the field of internet communication in the last decade worldwide have crossed all the physical boundaries laid down by human being and this era witnessed a major development in the field of Information Technology and made a large number of computer users in the world. Every common man is influenced by this new world of communication named as cyber world. But there are always two aspects associated with every technology; the destructive side is threats associated with this internet communication in cyberspace. A rapid growth of computer crimes and formation of laws in different countries addresses the severity of problem. This paper discusses the stand of Saudi Arabian government against cyber crime and its IT act. It analyzes the cybercrime in the Kingdom and the associated legislation to combat the same.**

Index Terms**: Computer Crime; Cyber Laws; Pornography; Cyber Terrorism; Anticrime Act.**

I. INTRODUCTION

Computer crime includes the crimes that act via computers. The computer may be used in the commission of a crime, or it may be the target. There are various types of computer crimes [1]:

A. Hacking

Hacking means illegally entering to the system to destroy or steal the information from that system. The hacking may be on the personal computer or on the governments system. Hacking is usually done by the employees who are disgruntled from their job. This may cost the company more damages like stealing information from this company or steal the account information of the company and may be it lead to destroy the company. This crime falls under the penalty of theft, the primary objective is to steal information. That crime can cause great damage and significant losses.

Naasir Kamaal Khan, *Department of Computer Engineering, Jazan University, Jazan -114, Kingdom of Saudi Arabia, Phone 00966557804924*

B. Pornography

It means the emergence of the females and children in pictures or videos of a porn nature or sexual movies to sexually abuse the humans. This crime is punishable by all the nations because of the danger to the children and its impact on the lives of social community. There is a clear tightening of all societies, whether Islamic or the Western on this crime and in their laws there are a harsh punishment of this type of crime especially in the UNICEF organization which it showing a big care of this crime and imposed their own laws and committed all the countries to apply them.

C. Denial of service Attack

DOS attacks give hackers a way to bring down a network without gaining internal access. Denial of services attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).

D. Virus Dissemination

Viruses and worms are usually made to destroy data in the computer. It is usually sent by hackers through e-mail but there are another ways like when you download a program or video they can put the virus with download data or they can sending it through the messenger programs such as Hotmail or Yahoo messenger.

E. Software Piracy

The **copyright infringement of software** (often referred to as **software piracy**) refers to several practices which involve the unauthorized copying of computer software. Copyright infringement of this kind is extremely common. Most countries have copyright laws which apply to software, but the degree of enforcement varies [1]. There are organizations called Anti-Copyright Infringement Organizations they give the ownerships to copyrighters and save their work software like: Business Software Alliance (BSA), Canadian Alliance against Software Theft (CAAST), Federation against Software Theft (FAST), International Intellectual Property Alliance (IIPA).

F. Website Defacement

It is meant to create a website on the internet to disseminate pornography via using porn videos or pictures. It also includes creating a website for trade of the wrong things.

G. Amateurs

These hackers send a virus or try to destroy the system for making just for fun, but he may be go far from this limit and try this with a governments system like the one who enter to

education system and change sensitive information related to student data.

H. Cyber Terrorism:

Terrorism is one of the major problems of this time. The only goal is to destroy the country's security and make the people scared. This includes making websites on the internet to communicate with their organizations or they explain how to make explosives or any tool that can use it in a terrorism operation or those who propagate nuisance. This crime falls under the category of major crime because it threatens the security of country.

I. Illegal Trade via Internet:

It is the creating a website in the internet to trade on illegal substances like (Drugs, Weapons or Alcohol) or it makes it easy to dealing with.

J. Phishing:

It is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

II. CYBER CRIME IN SAUDI ARABIA

Information Technology highly influenced the Arab world in the last decade which results in increase of Internet users day by day. Almost all countries in the Middle East have cyber laws. The large population of Muslims in this world requires establishing a law suitable to handle cyber crimes that matches the Islamic law. Generally Computer crime initiated from pirated software, Internet relay chat and other small scale acts but severity happens when it grows to hacking a financial or governmental system. Almost all of the governmental transaction in Saudi Arabia involves computer whether it is traffic control, Telecom & Electricity, Health Information System or Passport, any breach in the security of Government system can result in serious harm and all their stored data is at stake. E-crime is part of or involved in all 'traditional crimes' such as drug trafficking, people smuggling and money laundering [2]. What is really threatening is that youth are involved in such crimes and they generally do not hesitate to use the Internet to commit different types of crimes right from copying data to drug promotion and pornography. Also due to global nature of computer crime it is really challenging to deal with it. There are a number of computer crime laws developed by many western countries, for example Texas Computer Crime Law [4]. Section 33.02 in Texas Computer Crime Law defines the breach of computer security in several points. Although that there are commonalities between a cyber and a physical crime scene, there are also significant differences [3], making the topic of cyber-crime an important area of research. This has been acknowledged by European governmental agencies; see for example the UK's Parliamentary Office of Science and Technology Report [5]. The main difference is that the boundaries of a digital crime scene are not clearly defined and the crime scene area may extend beyond a building, region, country, or a continent. For instance, a computer virus outbreak may impact a large proportion of computers connected to the Internet. Formally, the crime scene would then be defined as the area that includes all infected computers. Alternatively, an identity thief or a pedophile may use a remote server to host illegal material and that server may be miles away from the person's physical location. In this case, the crime scene would be the person's physical location, the remote server, and the network paths that the relevant network protocols utilize.

III. THE ANTI-CRIME ACT IN SAUDI ARABIA

Legislation is the back bone of every society. Laws along with moral ethics can make world peaceful and free from any nuisance. It is the key to form secure society and makes the country a suitable place for living and connecting with the others. Since cybercrime is a problem and a threat to social life, so it is very necessary to have laws of its own and be a deterrent to the perpetrator of these crimes. In Saudi Arabia there is a special case in that the sanctions imposed as punishment are approved as stated in the Qur'aan and Sunnah [6]. And the Holy Qur'aan did not mention the laws and penalties for computer crimes, but said public sanctions such as theft, murder, adultery and other sanctions, so an Anti-Crime act is there to combat cyber crimes. It also determines the level of each crime and the resulting harm. For example (Theft of bank accounts and theft of the personal pictures or videos from computer) they are fall under the theft low but there are different effects of each one, so the consequences of each one of them must be different. In the laws of all country the age of children should be less than 18 but in Saudi Arabia there are 15 members of the Shoura Council which suggest that the age of children should be less than 15. In Saudi Arabia there is a study that shows 20% of the children exposed to pornography crime every year [8]. Some websites published pornography and scratch the Islamic values, are blocked as managed by Internet Services in Saudi Arabia (www.internet.gov.sa). Cyber Terrorism crime falls under spreading corruption. Research about computer crime and computer ethics are two faces of same coin. The ability of writing on computer ethics and associated areas to make a deeper understanding of inequalities surrounding in the field of information technology is highly affected by forms of technological determinism and liberalism [9]. Computer crimes can take many different forms, from cyber stalking to child pornography [10]. Cyber stalking describes stalking behavior executed by means of some aspect of information technologies. The ever increasing use of the Internet by 'criminals' has prompted a rush of legislation and other interest [9]. Unfortunately, despite a number of high-profile cases reported both in print media and on the Internet, the topic has yet to receive systematic analysis against an appropriate theoretical framework [11]. Such a theoretical

framework must include a combination of an understanding of the psychological phenomenon of stalking, an understanding of Internet crime. Some people may argue that our rights of privacy are "socially constructed," means that they change over time under the influence of many human forces and institutions, including technology, culture, and law [11].In the year 2007 Saudi Arabian government introduces Anticrime act. Following are the computer crimes and Sanctions proposed [7]:

Table I: Anti Crime Act 2007

No.	Type of Crime	Penalty
1	Hacking, Net Extortion, Website Defacement	SR 5,00,00 or 1 Year or both
2	Spoofing, Credit Card Fraud	SR 20,00,000 or 3Years or both
3	Denial of Service, Software Piracy, Data Diddling	SR 30,00,000 or 4Years or both
4	Virus Dissemination, Pornography, Illegal Trade	SR 30,00,000 or 5 Years or both
5	Cyber Terrorism	SR 50,00,000 or 10 Years or both

IV. DISCUSSION

It has been observed that since the last decade due to tremendous increase in number of computer users cybercrime has been increased anonymously. The basic cause behind this is non awareness of laws in Saudi youth as the major population of Internet users are University students, boys and girls. Cyber laws exist in the Kingdom since the year 2007, but its non awareness among youth has created potential imbalance between safe internet usage and vulnerability against crime. Government has taken control on many porn internet sites which are prohibited to open in the Kingdom. A central server manages the filtration and pornography is avoided almost all the time. But at the receiving end the scenario is a bit different, potential users are unaware of laws and penalties associated with cyber crime. Most of the people know about cyber crime but very less is aware of the associated legislation to combat these crimes. The detail of penalties is a far story for almost all of them.

V. CONCLUSION

Saudi Arabia is an Islamic country and follows law of Sharia'h. Many crimes are avoided due to Sharia'h law and fear of God. The Information and communication Technology in cyber world has given a challenge to all as there is no trace of cyber crime and may be no evidence. Muslims always try to relate to Islamic teachings which instill the fear of God and hence the main conclusion of this research is to debate about non awareness of law and potential imbalance between Internet Usage & Awareness program in Kingdom. The ruling in Saudi Arabia is based on Islamic Law so the main problem is non awareness of laws and absence of cyber crime education among Saudi youth, as laws are also based on Islam which addresses the individual before the crime is committed and hence is more necessary the prevention than a cure. Security vulnerability analysis shows that the major population is still unaddressed.

REFERENCES

[1] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0201707195.
[2] DTI/PWC (2004). *Information security breaches survey*. London: PWC.
[3] T. Chen, C. Davis, An overview of electronic attacks, in: P. Kanellis (Ed.),
Digital Crime and Forensic Science in Cyberspace, Idea Group Pub., London, 2006, pp. 1–26.
[4] Texas Computer Crime Law (1994). Retrieved September 15, 2007, from http://suefaw.home.texas.net
[5] Parliamentary Office of Science and Technology, POST. Computer Crime. POSTnote, N. 271, (2006) available from: http://www.parliament.uk/ documents/upload/postpn271.pdf
[6] The Holy Quran.
[7] Madkoar, M.S. (1980). *The Effect of Islamic Legislation on Crime Prevention in Saudi Arabia*. Ministry of Interior, Kingdom of Saudi Arabia, (In Arabic).
[8] Ministry of Justice.
http://www.moj.gov.sa/adl/ENG/attach/28.pdf last accessed 10/10/2012.
[9] Alison, A. (2001). Computer ethics in a different voice. *Information and Organization*, 11, 235-261.
[10] Newman, G., & Clarke, R. (2003). Superhighway robbery: Preventing e-commerce crime. Portland, Oregan: Willan.
[11] Levine, P. (2003). Information technology and the social construction of information privacy: Comment. *Journal of Accounting and Public Policy*, 22, 281-285.

Naasir Kamaal Khan has received his B.E (Hons.), M.Tech (IT) and pursuing Ph.D in Information Technology. Presently he is working at College of Computer and Information System, Jazan University. Over the span of 9 years of his teaching experience he has Published & Presented Several Research Papers in National & International Conferences, Delivered expert lectures in India & Abroad. He has supervised several student research projects. He is a Life Member of Indian Society of Technical Education (ISTE). His areas of interest are Cryptography & Network Security, Information & System Security and Computer Networks.