American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-10, pp-253-257
www.ajer.org

Research Paper Open Access

Cyber laws encompassing the Security of E-Quran in Saudi Arabia

Naasir Kamaal Khan
Department of Computer Engineering, Jazan University, Jazan, Kingdom of Saudi Arabia

Abstract: - Past two decades in the world have seen tremendous growth in the use of Information Technology in almost every field of daily life. We have seen abrupt changes in the society and paper world is completely changed to electronic world. The use of electronic format of storing, processing and retrieval of data made ease for the human kind in a multidimensional way which influences the human being in all the aspects of life. The growth of using Holy Quran for reading and learning through electronic mode is increasing day by day. As there are always two faces of a coin, the other side shows the risks and vulnerabilities associated with the use of e-Quran. With over 1.5 billion of Muslim population in the world, several calls were raised in the Islamic countries to establish a law suitable to handle computer crimes which matches the Islamic Shariah law. In this paper threats associated with the use of digital format of Quran and existing cyber laws associated with it, are discussed, both in the Kingdom and worldwide. The author conducted on extensive review of published literature on a number of computer crime laws developed by many countries, which includes Texas Computer Crime Law, Anticrime act 2007 of Saudi Arabia and cyber laws in other countries of Middle East. Lastly author proposes the amendments in the latest version of Cyberlaws for securing the Holy Quran, in the light of present Anticrime act of World especially in Middle East as computer crime is of a global nature and the present penalties associated with Modification and fabrication of electronic data is not enough when we talk about the holy book Quran.

Keywords: - *Piracy; Cyber Laws; Texas Law; Islamic Law; e-Quran.*

I. INTRODUCTION

Information Technology is rapidly growing field in the modern era. The electronic form of data storage, processing and retrivel has completely removed the paper world. The use of data in electronic form facilitates its user to carry it anywhere without any intervention of physical boundry. The compulsion of size and space has also been vanished. But the darker aspect of this technology has also a great impact, which can not be neglected.Tremendous growth in computer and Internet users since last few years increases the problem manyfold. Computer is now not limited to corporate, business or education world, it has been reached to each individual in one form or another which leads to unauthorised access of digital data.

This unauthorized creation and distribution of any software is considered as software piracy. The origin of software piracy lies in the early 1960s, when computer programs were freely distributed with mainframe hardware by hardware manufacturers. In the late 1960s, manufacturers began selling their software separately from the required hardware [1]. Some file sharing programs like ‘bit torrent’ and ‘napster’ are also contributing in software piracy. According to the BSA statistics, the piracy rate is increased from 2% to 43% in short span, just because of the highly demanded PC market in developing countries [2]. People in the world get used to install and download false materials and products and also feel happy to be able to afford these materials without any cost and resulting harm to the individual or masses [3].

II. THREATS TO E-QURAN

Computer crime by definition means where computer is used as a target, tool or both. Threats associated with computer are classified as Interception, Interruption, Modification and Fabrication. Out of which Modification and fabrication is the severe one which attacks on Integrity of data. As transmitting and receiving the data in electronic form does not follow any physical rule due to anonymity of source, it is difficult to track the

malpractice easily. But laws can be incorporated as soon as malpractice is detected and the culprit can be punished. Hackers are continuously identifying new means of stealing information. Unfortunately, the presence of unaware users in an environment surrounded by digital world makes them an easy target for hackers. User education and training is a must to combat computer security threats. This is not a simple task to achieve and not the sole responsibility of the user or the organization. Many groups have to be involved to produce an IT security-aware resident [4].

The electronic use of Quran is common now a days, whether it is through Desktop PC, Tablet or Smart phones. The e-Quran is also vulnerable to various attacks including the most severe one, which is attack on Integrity. There are several threats and vulnerabilities to e-Quran which can be classified broadly in two categories. First, Fabrication of false e-Quran from scratch and secondly Interception and modification in authenticated copy of e-Quran. The first category falls under integrity of the content which closely resemble with the financial and banking data. Spoofing and Masquerading are two types of attack which talks about integrity but usually ignored in cyber crime dictionary and assumed to be less harmful crime. The word spoof means to deceive. In digital world spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

The second category falls under confidentiality of data, software piracy is popularly known crime in this category. Term Data diddling is also used for small alteration of data Masquerading is an attack by which a person claims to be another person and takes all the privileges available in that IP-address. Data diddling is a man in the middle attack where the MITM not only intercept the data but also alter the data. Diddle means a small change in setting to bring your system down, like in buffer overflow attacks. [5]

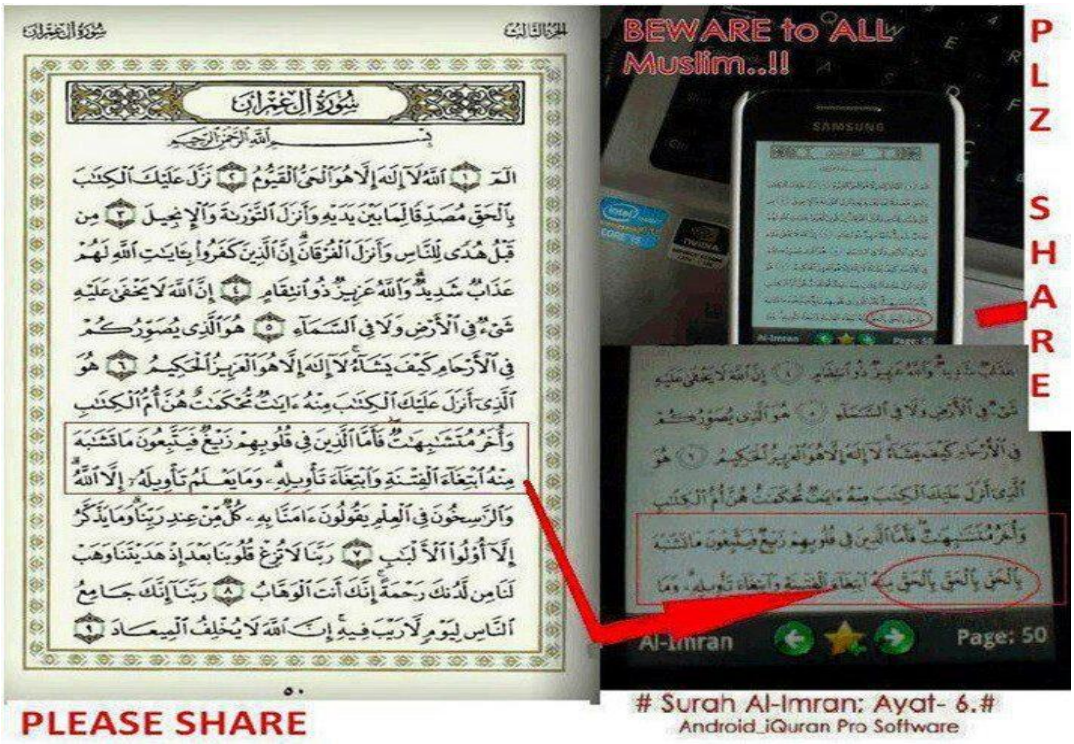

Figure 1 - Integrity Attack (retrieved from Facebook)

III. EXISTING CYBER LAWS

Most the countries across the globe have cyberlaws based on their requirement, culture and ambience. In Islam the basis of law is Quran and hadith and cyberlaws are also replica of the same. In section 33.02 of Texas cyber law [6] breach of computer security is described under several parameters of personal and financial security. U.S cyberlaws [7] states in section 18 U.S.C. § 1028 about Fraud and related activity in connection with identification documents, authentication features, and information, section18 U.S.C. § 1028A about Aggravated identity theft and 18 U.S.C. §§ 2516 about Interception of wire, oral, or electronic communication i.e piracy.

The study of present cyber legislation of all the Economic and Social Commission for Western Asia (ESCWA) members, namely: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, the Syrian Arab Republic, the United Arab Emirates and Yemen shows the flaws and shortcoming in existing laws [8].

In this paper three major countries of Middle East namely Saudi Arab, Oman and UAE are taken into consideration and their laws related to above mentioned two categories are being analyzed.

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Republic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Mauritius	✔	✔		✔	✔	✔	✔	✔	✔	
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

Figure -2. Countries with Updated Law [8]

A. Cyberlaws of United Arab Emirates

Article 10 of UAE cyber laws [9] states that penalty of Impersonation, masquerading or fraud is imprisonment for a term of at least 1 year and fine of at least AED 30,000 or either. Article 15 states that the penalty of imprisonment upto 7 years for following crimes through computers

- Abuse of an Islamic holy shrine or ritual
- Abuse of a holy shrine or ritual of any other religion where such shrine or ritual is protected under Islamic Sharia.
- Defamation of any of the divine religions.
- Glorification, incitement or promotion of wrong doing.

B. Cyberlaws of Oman

Chapter Four of Oman Cyber laws [10] named Forgery & information Fraud states in Article 12 that the penalty with imprisonment for a period not less than one year and not exceeding three years and a fine not less than OMR one thousand and not exceeding OMR three thousands or by either penalty, shall be applied to any person who uses the information technology tools in the commission of informational forgery crimes by changing the nature of such data or the electronic information by addition or deletion or replacement with the intent to use it as proper data or electronic information, acceptable in an informational system legally a matter which might causes personal benefit to him or the other or causes damage to the other. If such data or electronic information is governmental, then the penalty shall be temporary imprisonment for a period not less than three years and not exceeding fifteen years and a fine not less than OMR three thousands and not exceeding OMR fifty thousands. The same punishment provided for in the previous paragraph shall be applied mutatis mutandis to any person who knowingly uses the forged data or electronic information.

In Article 19 The penalty with imprisonment for a period not less than one month and not exceeding three years and a fine not less than OMR one thousand and not exceeding OMR three thousands or by either penalty, shall be applied to any person who uses the informational network or the information technology facilities to produce or publish or distribute or purchase or possess whatsoever that might prejudice the public order or religious values.

C. Cyberlaws of Saudi Arabia

Article 6 of Saudi Arabia Cyber law [11] states that Any person who is involved in Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding three million riyals or either.

IV. PROPOSED AMENDMENTS TO EXISTING LAW

Existing Cyberlaws all over the world addresses integrity issue of data storage, processing and retrival. It includes software piracy and intellectual property right, but nowhere laws are made specifically against malpractice or fabrication of religious scripture including UAE, Oman and Saudi Arabia.

In Surah Baqarah, from ayat 78 to 81 (2:78 to 2:81) Allah says that **"**Among them are unilletrate ones who do not know the Scripture except in wishful thinking, but they are only assuming. So woe to those who write the

"scripture" with their own hands, then say, "This is from Allah ," in order to exchange it for a small price. Woe to them for what their hands have written and woe to them for what they earn. And they say, "Never will the Fire touch us, except for a few days." Say, "Have you taken a covenant with Allah ? For Allah will never break His covenant. Or do you say about Allah that which you do not know?" Yes, whoever earns evil and his sin has encompassed him - those are the companions of the Fire; they will abide therein eternally." So the penalty of modification and fabrication of Quran should not be less then capital punishment as the intruders not only doing a crime of diddling text whether intentionally or un-intentionally but also spreading mischief to Innocent and unaware computer / smartphone users.

Author advocates that the ammendments should be done in cyber laws as the present laws are insufficient and weak. So more stronger laws should be included at least in arab world to protect integrity of e-Quran. The penalties to the criminal should not be less then the Drug traficking or Cyber Terrorism.

In author's view this crime should come in the category of content crime in present Omani Cyber Laws [10], where the penalty is life imprisonment and a fine of one hundred thousand OMR or as in Article 25 where the punishment is the death penalty or life imprisonment and a fine of twenty five thousand OMR. In Saudi Arabian cyber laws [11] this crime should come under Article 7 where imprisonment is for ten years, and a fine of five million riyals.

In this context Author Proposes following Amenmends in the present Cyberlaws :

1. *A Separate Article in the law should be made against foregery of e-Quran.*
2. *This Article should be subdivided in two categories; Fabrication of e-Quran and Modification of e-Quran.*
3. *For Fabrication the penalty should not be less then life imprisonment.*
4. *For Modification the penalty should not be less then ten years of imprisonment and fine of five million riyal.*
5. *In both the cases criminal should be banned to use computer and Internet for a lifetime.*

V. DISCUSSION

Legislation is the back bone of every society. 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. There are public sanctions such as theft, murder, adultery for which an Anti-Crime act was introduced in 2007 to combat cyber crimes. It also determines the level of each crime and the resulting harm[12]. In [4] some recommendations were given such as formation of Computer Emergency Response Teams (CERT) to enhance the security awareness among residents. Involvements of Police Departments, Enterprises, Telecommunication companies (ISPs), Media and Users.

In 2008, a new initiative has been proposed to fight cyber terrorism by bringing governments, businesses, and academia together from all over the world. The initiative, known as the International Multilateral Partnership Against Cyber Threats (IMPACT) [13], consists of the international partnership of more than 30 countries to study and respond to high-level cyber security threats.

Apart from the common legislation of cyber crime in Kingdom, it is now important to have a special law to protect integrity of e-Quran. It is observed in the near past that the smart phone users are increasing day by day and several versions of software of e-Quran is now available. So the chance of forgery and fabrication also increases proportionally. A common user can easily be misguided due to unawareness of this fraud. An example of "Musaylimah bin Ḥabīb" alias Kazzab belonged to tribe Banu Hanifa used to compose verses and offer them, as Quranic revelations. Most of his verses extolled the superiority of his tribe, the Bani Hanifa, over the Quraysh [14]. He was killed in the battle of Yamama and later his followers were executed. There are many hidden culprits in cyber world now a day's who intentionally spread mischief in the land so it is necessary to make strong law to protect Holy Scripture in electronic form.

In Figure 3 it is shown that any security system cannot be established until it is supported by three features, viz. Selection of Control policies, Implementation and Monitoring. So to have a strict law it is recommended to have all these features incorporated in the system.

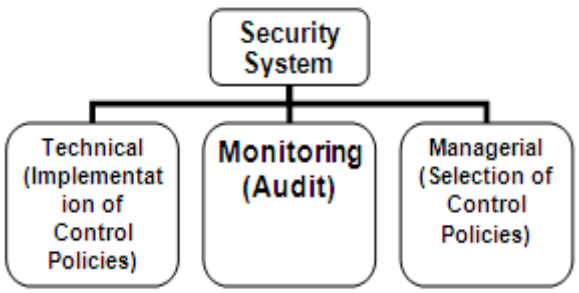

Figure 3 - Security System features

VI. CONCLUSION

In this paper several forms of cybercrime were discussed especially those are connected to piracy and fraud. A correlation has been made of these crimes with the threats of e-Quran and various other threats were also discussed. After analyzing threats to e-Quran they were categorized in two broad fields, modification and fabrication which challenge the integrity of e-Quran. Existing laws related to piracy and forgery were discussed in general and related to e-Quran in particular in the cyber laws of many countries particularly UAE, Oman and Saudi Arabia. It was observed that any of the three does not include any clear law to protect e-Quran. Author proposes some amendments in the existing law and advocated to have stronger law for security of e-Quran as it is matter of faith, religion and moral values. Lastly some case studies were discussed related to this research with managerial, social and technical aspects.

VII. REFERENCES

[1] Business Software Alliance, "Eighth annual BSA global software 2010 piracy study", May 2011.

[2] Ajay Nehra, Rajkiran Meena, Deepak Sohu, and Om Prakash Rishi. "A Robust Approach to Prevent Software Piracy".Students Conference on Engineering and Systems (SCES), IEEE 2012.

[3] Samir N. Hamade. "The Legal and Political Aspects of Software Piracy in the Arab World" Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), IEEE 2006.

[4] Fadi A. Aloul."Information Security Awareness in UAE: A Survey Paper". IEEE International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, pp. 1-6, November 2010.

[5] CAPEC; A Community of knowledge resource for building secure software, available online at http://capec.mitre.org/data/definitions/184.html

[6] Texas Computer Crime Law. Available Online: http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.33.htm

[7] Cybercrime Laws Of The United States. Compiled October 2006 by Al Rees, CCIPS. http://www.qcert.org/sites/default/files/public/documents/us-ecrime-compilation_of_cybercrime_laws-eng-2006.pdf Last accessed on 1/7/2013

[8] Models of Cyber Legislation ESCWA Countries. Available online at http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf.

[9] The Federal Law No. (2) of 2006 on The Prevention of Information Technology Crimes published in the Official Gazette of the United Arab Emirates, Volume 442, 36th year, Muharam 1427 H/ January 2006.

[10] Cybercrime Law Sultan of Oman, Royal Decree No 12/2011; English Version available online http://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf .

[11] Anti-Cyber Crime Law of Kingdom of Saudi Arabia. Bureau of Experts at the Council of Ministers Official Translation Department Translation of Saudi Laws, 8 Rabi1, 1428 / 26 March 2007.

[12] Naasir Kamaal Khan. "Taxonomy of Cyber Crimes and Legislation in Saudi Arabia" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) ISSN: 2278-1323 Volume:1, Issue:8 October 2012, page 207-209.

[13] International Multilateral Partnership Against Cyber Threats (IMPACT), available online at www.impact-alliance.org/

[14] The Life of the Prophet Muhammad: Al-Sira Al-Nabawiyya By Ibn Kathir and Muneer Fareed.