Cyber Crime an Emerging Challenges for Law Enforcement Agencies of 21st Century: An Appraisal with Islamic Perspective

Md. Shahadat Hossain*

Abstract

This article is concerned with the crimes occurred in virtual space, which are the emerging challenges to the law enforcement agencies of this globe and Islamic response for combating such crimes. This paper also examinee the verity of cyber crimes with the traditional offences of similar nature and identify the criterion of punishment that would be appropriate for particular crime. It further expresses the limitations of Islamic research on this topic and encourages to study about the critical legal processes which are subject to improvement such as admissibility of electronic documents, procedure for execution of ÍudËd, QiÎÉÎ and TaʽzÊr punishment for cyber offences. This paper highlighted the cyber security challenges and Islamic perception of cyber crime along its mechanism for combating such high-tech criminal activities.

Keywords: Cyber Space, Cyber Crime, Challenge, Law, and Islam.

1. Prologue

Ever since the dawn of human civilization crime has been an impenetrable problem. There is hardly any society, which is not overwhelmed with the dilemma of crime and criminality. Crime is inevitable in any human society since some contravention or the other of any code of conduct prescribed for members of a society is bound to occur.[1] The inevitability and universality of the phenomenon of crime has been described by Emile Durhkheim in the following words "There is no society that is not confronted with the problem of criminality. It's from changes; the acts thus characterized are not the same everywhere; but, everywhere and always, there have been men who have behaved in such a way as to draw upon themselves penal repression."[2] They, therefore, are continuously searching the etiology of crime, which may

be, in different classification.[3] Cyber crime is the most recent criminal bustle across the globe, which caused massive destruction and irreparable loss to the victim. Cyber crime at the 21st Century is required to unbolt the new jurisprudential explanation, which attributes the modification and wide application of laws for combating the high-tec offences around the world. Islamic criminal jurisprudence does not remain silent in the matter concerned. Penology and the principle of Islamic criminal justice administration have strengths to address the issues like this. In this manuscript, we would like to expose the directions of Shariah as regards the cyber crime and its deterrence.

2. Identifying Cyber Space

Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. Cyberspace is a virtual space which is not confined to any territorial boundaries or limits and such virtual space belongs to all who have the capability to utilize it for their development. Cyberspace is the global domain of electromagnetic in nature; the electronic medium in which communication and control is executed through the modulation of electromagnetic energy across specified networks.[4] It is readily identified with the interconnected information technology, which is required to achieve the wide range of system capabilities associated with the transport of communication and control products and services. The term "cyberspace" was first used in the 'Cyberpunk science fiction' by William Gibson.[5] The term is evocative and essentially meaningless and buzzword that could serve as a cipher for all of his cybernetic musings. Now ubiquitous, the term has become a conventional means to describe anything associated with computers, information technology, the internet and the diverse internet culture. Cyberspace is a consensual hallucination experienced daily by billions of legitimate operators, in every nation. The symbol used to describe the "sense of a social setting that exists purely within a space of representation and communication… it exists entirely within a computer space, distributed across increasingly complex and fluid networks".[6] It extends across immense region of electron states,

---

* Md. Shahadat Hossain, Lecturer, Department of Law, Bangladesh Islami University, Dhaka, Bangladesh.

[1] S.M. Afzal Qadri, Criminology, 5th edn., (2005), p 1.

[2] Emile Derkheim, Rules of Sociological Method, (1950), p. 65.

[3] Sheik Hafizur Rahman Karzon, Theoretical and Applied Criminology (n.p. 1st edn, 2008), p. 1.

[4] Free Dictionary at: http://www.thefreedictionary.com/cyberspace "Cyberspace Defined"

[5] William Gibson, Neuromancer (New York: Ace Books, 20th Anniversary Edition 2004), p.69.

[6] Don Slater, "Social Relationships and Identity Online and Offline", in L.Lievrouw and S.Livingston (edn.), The Handbook of New Media, Sage, (London: 2002), p. 533–46.

microwaves, magnetic fields.[7] Owing to the atypical nature of this virtual world with so many actual legal challenges, innovative legislative approach is chosen in many countries to maintain law and order.

3. Introduction to Cyber Crime

Computer crime is a multi-billion dollar problem. Law enforcement agencies must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cybercrime is a menace that has to be tackled effectively not only by the officials but also by the users by co-operating with the law. With the technological expansion, new shapes of crimes have taken birth, the latest and more dangerous being the cyber crime. Cybercrime refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of the crime. Cyber crime is one in which the computer forms the main weapon. The computer created by genius minds can now be used to commit various criminal offences. A creation of human beings, computers can be used for attaining new heights of success and can also be used as a weapon of crime. Cyber crimes are harmful acts committed from or against a computer or network. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It admits the surging enthusiasm and interest, however, runs a cavernous thread of ambivalence towards connecting to the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Most prominent form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb.[8] Cyber crime has set in a debate as to whether a new legislation is needed to deal with them or existing legal regime is flexible enough to effectively deal with the new forms of criminality.[9] There is a school of thought that believes that cyber crimes are not in any way dissimilar to the ordinary crimes.[10] Other schools expose that the nature of the emerging technologies and unique set of challenges are unknown to the existing criminal jurisprudence. Therefore, it contends that a new comprehensive legislation is needed to deal the cyber crime.[11]

4. Cyber Security Challenges

Computer crime or e-crime presents one of the major challenges of the future to law enforcement.[12] Cyberspace does not recognize geographical boundaries. This has proved a boon to the delinquents who perform illegal activities on the internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the law enforcement agencies further complicates the matter.[13] Computer sanctuary and associated crime is increasingly becoming a foremost concern for the corporations and government organizations. Law enforcement in the nations throughout the world has tolerated many challenges over the years. While committing the crime, perpetrators have integrated highly technical methods and developed crimes of innovative nature. Moreover, the evidence of these crimes is neither human nor physical, rather electronic impulses and programming codes. It is, therefore, very difficult to put those activities under the general purview of the existing legislations. Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of business and as an emerging threat to the nations' safeguard.[14] The challenges pretended by cyber crimes are classified. First, legal challenges, which are dependent on the statutory provisions to be used as a tool to investigate and control the cyber crimes. Secondly, operational challenges require a cohesive

[7]   John Perry Barlow, Crime and Puzzlement, http://www. Wikipadia.org.
[8]   National Research Council, "Computers at Risk", 1991. Online source: http://www.crime-research.org/analytics
[9]   Dr. Farooq Ahmed, Cyber Law in India (Law on Internet) (2nd edn., 2005), p. 300.

[10] Watkins, "Computer Crime: Separating the Myth from Reality", in C.A. Magazine, (Jan. 1981),
[11] Parker, Computer Abuse Research Update (1980), p. 329-523. See also: Michael A. Sussman, The Critical Challenges from the International High- Tech and computer-related Crime at the Millennium (FUKEJ. COMP & INLT L. 451, 1999), p. 453-55.
[12] Backhouse, J., & Dhillon, G., Managing Computer Crime: A Research Outlook. Computers and Security, 14(7), 1995, p. 645–651. See also, Dhillon, G., & Moores, S. Computer Crimes: Theorizing about the Enemy within. Computers and Security, 20(8), 2001, 715–723. Reference has been taken from 'Cybercrime and the Law: An Islamic View' by Mansoor Al-A'ali, Webology, Volume 4, Number 3, September 2007.
[13] Dr. Farooq Ahmed, Cyber Law in India (Law on Internet), (2nd edn., 2005), p.305.
[14] McConnell International, Cyber Crime . . . and Punishment? (Archaic Laws Threaten Global Information, 2000) at: www.mcconnellinternational.com.

well-trained and well-equipped force of investigators operating and coordinating at national and international level. Thirdly, technical challenges thwarting the efforts of law enforcement agencies' ability to catch and prosecute the online offences.[15] As we mentioned earlier that Cyber crimes are often committed beyond the national borders. It is very, difficult to identify the perpetrators because of internet facilities anonymity. These crimes cannot be effectively dealt with simply passing national legislation. The Act has extra territorial jurisdiction and applies to any offence or contravention thereunder committed outside the country by any person. This feature of the Information Technology (IT) legislation is not unusual. Similar provision is found in IT laws of other jurisdictions also.[16] Cyber security can be effectively maintained when the concerned laws have a massive deterrence and enclose applicability in a wide assortment. Eventually, a mutual cooperation at the international level amongst enforcement authorities and Government is required.

5. Perception of Crime and Criminals in Islam

The terminologies used in the Qur'Én and Sunnah to denote crime and criminal activities are jinÉ'iah, jarÊmah and jarÊrah. The terms literally mean crime, to commit an offence, a sin, an act of disobedience, a misdemeanor, a transgression, to cut off etc.[17] The word Jurm has been used for unfair earning and unfair action. It has been used in the same sense in the holy Qur'Én and derives from these verses that all actions that are against justice and right path are called jurm or crime.[18] All the directions of SharÊ'ah are fair being the directions of Allah and his Messenger (p.b.u.h.) and thus their disobedience amounts to jurm or offence.[19] The word jurm signifies to do what has been prohibited in SharÊ'ah or not to do what has been ordered by Shariah to be done and for which punishment of ×add or Ta'zÊr has been prescribed.[20] JinÉiah primarily means the act of gathering, plucking or taking fruit from a tree,

an evil thing or actions, doing a forbidden action.[21] JinÉiah, therefore, technically means any unlawful actions, which cause physical injury to an individual, or harms and annihilate the life and property of human being.[22] JinÉiah are of three types, first, JinÉiatu 'amad or willingness to commit crime or intentional offence, which means a desire to employ any device or weapons to commit a murder which usually use to commit a murder and hence commit the same through such weapons. Secondly, JinÉiatu Shibhi 'amad which is similar to intentional offence means an intention to commit a murder with any unusual means. Thirdly, JinÉiatul khaÏÉ' or crimes for mistake, it refers to commission of murder mistakenly, through any means.[23] Therefore, crime is an offence, which meted out with appropriate penalty and punishment.[24] According to the majority of the jurists, JinÉiah signifies all kinds of prohibited and injurious actions whether they relate to human body or property or other violations.[25] Al-MwardÊ described that crimes are wrongful acts in Sharia for which punishment has been prescribed by Allah whether Íadd (fixed punishment) or Ta'zÊr (discretionary punishment).[26] Wrongful acts are those which adversely affect the rights of an individual or the society or interfere with the peace and tranquility.[27]

The term Mujrim means perpetrators of offenders, criminals etc. At the day of resurrection, Almighty Allah will order to separate the (MujrimÏn) criminals, polytheists or wrongdoers from non-criminals or good dowers[28] and establish justice for all in accordance with their evil or well deeds. Islamic criminal jurisprudential perception regarding crime and criminals is that the comprehensive system of belief in the unseen, accountability on the Day of Judgment and Allah's Own Guidance about right and wrong makes the behavior and living of a man quiet distinct from the one having any other conception about man's status in this universe. This concept of man's status in the universe is the ultimate controller of the human behavior whether they perform good

15   S.S.H. Azami, Information Technology, Cyber Crimes and Solutions, Paper presented at International Conference on International Law in the New Millennium: Problems and Challenges, Ahead 4-7, October 2001.

16   Section 4 of the British Computer Misuse Act, 1993 (as amended 1998) and Section 9 of the Malaysian Computer Crimes Act, 1997.

17   Islamic Foundation Bangladesh, Arbi-bangla Abhidhan (Arabic to Bengali Dictionary) (Dhaka: Islamic Foundation, 2006), p.724-725 &754.

18   Al-Qur'Én, SËrah YaSin: 36:59, SËrah al-MÉ'Édah: 5:8; SËrah HËd: 11:89; SËrah al-Mursalat: 77:46; and SËrah al-MuÏaffifÊn: 83:29.

19   Anwarullah, The Criminal Law of Islam (Kuala Lumpur, n.d.), p. 2.

20   Quoted from: Ibid.

21   Edward William Lane, Arabic English Lexicon (Madd al- Qamus), Bk.1, pt. 2, 472. Quoted from: Ibid.

22   Mohhamad Quala'zi, Fiqh OthmÉn (Dhaka: Adhunik Prokashoni, 2002), p.151.

23   Ibid.

24   ABM Mahbubul Islam, "The Law of Islam is an Ultimate Solution Towards Crime-free Society: Special Reference to the Law of Retaliation", Bangladesh Islami University Journal (Dhaka: Bangladesh Islami University, July-December 2007), Vol. 01, Issue. 02, p. 13.

25   Abdul Qadir Awdah, Al-TashrÊ' al- JinÉ'Ê al-IslÉmÊ, vol.1.,p.65. Quoted by: Anwarullah, op. cit. p. 2.

26   Al-MawardÊ, Al-AÍ kÉm al- SulÏaniyyah, p. 192.

27   Anwarullah, op. cit. p.3.

28   AL-Qur'Én, SËrah YaSin: 36:59, SËrah al-Mursalat: 77:46.

deeds or commit crimes. Because those who do not consider themselves as answerable and responsible to Allmighty Allah, who act on this presumption that life is but of this world only, who measure one's success or failure according to the attainments in this world in respect of wealth, power and popularity, who depending upon their materialistic views reject the Allah's Guidance, do become a symbol of wickedness.[29] They live as if animals paying least regard to any moral values.[30] Hence, commit any sort of offences whatever they like and creates the whole universe into a hell for others.[31]

Muslim jurists have expressed that three basic elements are required for constitution of a crime and if any of these elements is missing the criminal shall not be liable to the punishment. First of all, legal elements which, mean an explicit provision for prohibiting an act constituting crime and declaring punishment thereof. Second one is the substantial element which means doing of an act which amounts to the commission of the crime and finally, cultural element which means the maturity, capability and accountability of the criminal.[32]

6. Crime and Punishment under Criminal Justice System in Islam
Under Islamic criminal jurisprudence, crime is constituted under the circumstances when certain primary rights of an individual are infringed. The term UqËbÉt denotes the punishment, which is found in numerous verses and traditions of the holy Qur'Én and Sunnah respectively along with the number of aspects. Infliction of several distinct punishments has also been directed in the above definitive sources of Islamic penal regulations. UqËbÉt is, therefore, concerned with the categories of criminal offences committed by the offenders against an individual in person, property, and honor or against the State and Religion or against the public peace, tranquility, decency and morality. Offences, which fall within the purview of the above-mentioned criterion, would be subject to condemnation irrespective of the division under which the offence is covered, that is ×udËd, QiÎÉÎ and Ta'zÊr sentences.

Among the division of punishment Hudud is ascertained and the offences are to be defined in the Qur'an and Sunnah, that is, adultery (ZinÉ), fornication (ZinÉ), false accusation (qadhf), apostasy (irtidÉd), drinking wine (khamr), theft (sarÊqah) and dacoity, robbery (qaÏ'at al-

ÏarÊq). These are the offences for which the punishment is fixed by the lawgiver and His messenger. Therefore, offences whether it follows the traditional ways like theft of jewelry form a jewelry superstore or using virtual mechanism like theft of currency through breaking the network systems of a bank, fall under the periphery of the above categories. QiÎÉÎ or retaliation is that punishment, which although fixed by the law, can be remitted by the person against whom the offence is occurred. It is applicable to cases of murder and wounding.[33] Retaliation, however, is inflicted upon those offences relating to murder and hurt. Eventually, Ta'zÊr is the form of punishment, which is subject to the discretion of the court or judges. Offences which are not in question to ×udËd and KaffÉrah would become the subject of Ta'zÊr sentences.

Discretion of the court has the wider scope of application of penalty to the crimes, seen and unseen. The opportunity for the exercise of such discretion must be the subject to the limitation of the SharÊ'ah and, therefore, it expands to the administration of criminal justice in a wide assortment. Non-traditional crimes like cyber crimes may be fall under the Ta'zÊr punishment except those, which, fall under ×udËd and QiÎÉÎ if matching. Exhibition of pornography, email harassment, email spoofing, unauthorized access to computer network etc. may fall within the purview of Ta'zÊr sentences. It is to be noted that whatever the characteristics of the crime, it must be identified by the law and subject to proof with proper evidences. In case of cyber crime, though there is no clear direction in SharÊ'ah, Islamic cyber law should recognize and plainly define the crimes and prescribe the punishment for particular criterion. In order to award sentences for such offences the complexity regarding admissibility of electronic evidences should be removed and appropriate provision made thereof.

7. Cyber Crime and Islam
Islam is an eternal apposite to all the ages of human civilization and demonstrates the illumination in every orb of the society for the betterment of its inhabitants with regard to safekeeping and tranquility. It would be a mysterious experience that the Islamic penal exposition remains soundless in administration of crimes occurred in the virtual space. Islam is, therefore, accustomed with comprehensiveness in stating the core principle of justice concerning the verity of aspects under which, all the traditional and extra-traditional crimes or cyber crimes is to be addressed. Cyber crimes have been categorized depending upon the

---

29 Muhammad Iqbal Siddiqi, The Penal Law of Islam, (1st edn., November 1979), p.3-4.
30 Al-Qur'Én SËrah al-A'raf: 7:179.
31 Al-Qur'Én SËrah al-RËm: 30:41.
32 Anwarullah, op. cit. p. 4.

33 Muhammad Iqbal Siddiqi, op. cit. p.52

nature and purpose of the offence and divided into three types concerning the target of crime. It may be against person, property and government.[34] The last category of cyber crime is popularly called as cyber terrorism.[35] David L. Carter has given the most comprehensive classification of cyber crime as crimes where computer is the target, where computer facilitates the commission of crime and where the computer is incidental to the crime.[36] However, we can summarise all the Cyber crimes in the following heads as Islamic law divides the crime concerns as well as the Islamic prescriptions to combat these criminal activities.

8. Cyber Crimes against Persons

Cyber Crimes that fall under the first category are: hate messages, stalking, defamation, harassment, launch of malicious program, espionage, spamming, e-mail threats, extortion, e-mail bombing, blackmail based on information gained from computerized files such as medical information, personal history, sexual preferences, financial data, denial of service attack, data diddling, unauthorized access to computer system, logic bombs etc. Islamic criminal jurisprudence addresses to those cyber crimes, which are associated with the nature of traditional offences and where the elements are available in the particular crime, though the methods utilized in the process is non-traditional in nature, must fall within the purview of Ta'zÉr regulations. Again, those offences, which are committed against any person and his honor, dignity, and reputation, will cover under Ta'zir punishment, because the lawgiver has not defined it, but left to the discretion of the judges of the court. Those offences, which contain the false and fabricated information in order to attract the target people to make them misguided regarding the originator of the information where he is not an actual maker rather used as a tool, fall under the umbrella of Ta'zÉr mechanism. Therefore, the SharÊ'ah preserves the opportunity to enact the laws for combating such offences. Qur'Énic response to such criminal acts is: "O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, do not spy on one another."[37]

9. Cyber Crimes against Property

This category covers offences like, theft of information, theft of passwords, theft of credit card numbers, e-mail bombing, insurance fraud, sale of pirated software, gambling, sale of stolen data, sale of stolen credit card number, Hacking the website of the corporations, fraud relating to electronic fund transfer, theft of intellectual property, theft of marketable information, sending virus or warm attack, theft of computer system, physically damaging of a computer system, denial of service attack, salami attack, Trojan attacks, money laundering, sale of illegal articles etc. Crimes which are committed against the property of a person or group of persons that is a company or corporation might come under the criterion of ÍudÉd, if the elements of theft are found. This amounts to an illegal misappropriation of others' property whatever the nature is. The Qur'Énic expressions to theft or misappropriation of properties are "O you who believe! Eat not up your property among yourselves unjustly except it be a trade amongst you, by mutual consent."[38] Again, the Qur'Én prohibits the greediness about the property of others "And wishes not for the things in which Allah has made some of you to excel others."[39] Further it is stated that no one should allow entering into another's property without his consent; "O believers! Do not enter houses other than your own until you have sought permission and greeted their inmates."[40] The expression, however, postulates that any types of misappropriation or theft of property or illegal access to computer network without the consent of others are to be treated as theft and therefore subject to ÍudÉd punishment. It is pertinent to note that one of the elements of theft is to obtain the ownership of the thing stolan by the thief. But in case of cyber theft the ownership may or may not remain with the owner or vice versa of the thing concerned. Therefore a new technical problem arises which requires the new jurisprudential interpretation to this attribute.

According to the verse of the SËrah al-×ujurÉt, Almighty Allah prohibits to spy on the secret to other. Secrecy has the wider application, which may include those hidden information inside the computer. In a tradition, the Prophet (peace be upon him) stated that "it is better for Muslim to mind his own business."[41] He further said, "Permission is for having a

[34] Farooq Ahmed, Cyber Law in India (law on Internet) (2nd edn., 2005), p.303.

[35] Arati Dubey, Cyber Law and Terorism, Souvenir, National Conference on Cyber Laws and Legal Education, NALSAR University of Law (2000) at 38. Quoted by Farooq Ahmed, op. cit. p.303.

[36] David L. Carter, Computer Crime Categories- How Techno-Criminals Operate (FBI Law Enforcement Bulletin, July 1995).

[37] Al-Qur'Én SËrah al-×ujurÉt: 49:12.

[38] Al-Qur'Én SËrah al-NisÉ': 5:29.

[39] Al-Qur'Én SËrah al-NisÉ': 5:32.

[40] Al-Qur'Én SËrah al-NËr: 24:27.

[41] Maik Bin Anas, Al-MuaÏÏÉ. (DÉr IÍyÉ' al-TurÉth Publishing,1980). Quoted by Monsoor al-A'IÉ, Cybercrime and the law: An Islamic (September, 2007), vol. 4, no. 3,

look."[42] These traditions focus on the point that a person is not allowed to show his curiosity on other peoples' business and can not have a look inside other person's properties if he did not allow him. Therefore we all know that the computer and its hidden information is a property. However, trespass to computer network system may be liable to Ta'zir punishment.

10. Cyber Crimes against Decency and Morality

Cyber crimes also attack the individual's morality. Crimes which fall under this category include: transmission and distribution of pornographic materials, sale of nude magazines, blackmail through factious sexual image, posting nude image to the friends using ones e-mail, using chat room to allure small children[43]etc. Indecent activities are extremely prohibited in Islam, which has been reflected in the holy Qur'Én as "Say (O Muhammad, peace be upon him) the things that my Lord has indeed forbidden are: Al-Fawahisha (great evil sins and every kind of unlawful sexual intercourse) whether committed openly or secretly, sins (of all kinds), unrighteous oppression, joining partners (in worship) with Allah for which He has given no authority, and saying things about Allah of which you have no knowledge."[44] In another place, holy Qur'Én directs "And come not near to unlawful sex. Verity, it is a Fahishah (that is anything that transgresses its limits: a great sin), and an evil way (that leads one to hell unless Allah forgives him)."[45] In considering the above Qur'Énic notion regarding fÉÍishah, it is clear that the offences occurred in cyber space, though these are not exactly as ZinÉ but it induce or provoke the mind of the user to commit such offences. Cyber pornography is the crime, which abets to commit sexual offences. Abetment is also prohibited in Islamic criminal law as; "help one another in Al-Birr and At-TaqwÉ (virtue, righteousness and piety); but not help one another in sin and transgression. And fear Allah. Verily Allah is severe in punishment."[46] Cyber crimes, which are involved with the obscenity and immorality induce adultery and fornication and are subject to be liable to Ta'zℏr punishment.

11. Cyber Crimes against State and Religion:

Since the offenders are highly skilled in using technology to do cyber crime, they target the government who is vulnerable in character or careless in the modern technology. Following offences fall under this type of cyber crime: threatening the government, cyber terrorism, unlawful access to government records, false and intentional propaganda against religion, publishing objectionable cartoon on religion and religious leaders etc. All conceivable offences against the State such as treason or public disorder or willful rebelliousness of the law of Allah using computer network system are also punishable by the holy Qur'Én as:

> "The punishment of those who wage war against Allah and His Apostle, and strive with might and main for mischief through the land is execution, or crucifixion or the cutting off of hands and feet from opposite sides or exile from the land; That their degree in this world, and a heavy punishment is theirs in the Hereafter. Except for those who repent before they fall into your power: in that case, know that Allah is oft-forgiving, most Merciful."[47]

In this verse the land refers to the territory of a country but the cyber crime has no any territorial limits. Therefore, the Islamic cyber regulations have extra-territorial application. Eventually the crimes associated with the nature of terrorism against the government and those, which address to the false propaganda against the particular religion, will be subject to the ÍudËd and Ta'zℏr punishment respectively.

12. Conclusion:

Cyber crimes have presented new challenges to the humanity in facilitating the innovative crimes, which have no specific boundaries and there may be no evidence to trace it. Despite the fact, Islamic penal laws are not silent regarding the matter concerned. Nevertheless, the problem is that neither we conduct research on this new dimension of crime nor we promulgate new laws addressing the cyber offences. This is the demand of the hours that we enact new Islamic cyber crimes laws in conformity with the internatiosnal initiatives.

---

[42]   Al-BukhÉrℏ, ØaÍℏÍ Al-BukhÉrℏ (Ibn Kathℏr Publishing, 1987. Quoted form: Ibid.

[43]   P. Rathore Subhas and B. Das Bharat, Cyber Crimes: The Emerging Trends and Challenges, Souvenir, national Conference on Cyber Laws and Legal Education NALSAR University of Law (2000) at 56-67. Quoted by: Farooq Ahmed, op. cit. p. 305.

[44]   Al-Qur'Én SËrah al-A'rÉr: 7:33.

[45]   Al-Qur'Én SËrah al-IsrÉ': 17:32.

[46]   Al-Qur'Én SËrah al-MÉ'idah: 5:02.

[47]   Al-Qur'Én SËrah al-MÉ'dℏah: 5:33-34.

References

Ahmed, Farooq. (2005). Cyber Law in India (Law on Internet) (2nd edn.).

Al-BukhÉrÊ. (1987). ØaÍÊÍ Al-BukhÉrÊ. Ibn KathÊr Publishing.

Anwarullah. (n.d.). The Criminal Law of Islam. Kuala Lumpur.

Awdah, Abdul Qadir. (n.d.). Al-TashrÊ' al- JinÉ'Ê al-IslÉmÊ. N.p.

Azami, S.S.H. (October 2001). Information Technology, Cyber Crimes and Solutions, Paper presented at International Conference on International Law in the New Millennium: Problems and Challenges.

Backhouse, J., & Dhillon, G.. (1995). Managing Computer Crime: A Research Outlook. Computers and Security.

Barlow, John Perry. (n.d.). Crime and Puzzlement. At: http://www. Wikipadia.org.

Carter, David L. (1995). Computer Crime Categories- How Techno-Criminals Operate. FBI Law Enforcement Bulletin.

Derkheim, Emile. (1950). Rules of Sociological Method.

Dhillon, G., & Moores, S. (2001). Computer Crimes: Theorizing about the Enemy within. Computers and Security, 20(8).

Dubey, Arati. (2000). Cyber Law and Terorism, Souvenir, National Conference on Cyber Laws and Legal Education, NALSAR University of Law.

Gibson, William. (2004). Neuromancer (20th Anniversary edn.). New York: Ace Books.

Islam, ABM Mahbubul. (2007). "The Law of Islam is an Ultimate Solution Towards Crime-free Society: Special Reference to the Law of Retaliation", Bangladesh Islami University Journal. Dhaka: Bangladesh Islami University.

Islamic Foundation Bangladesh. (2006). Arbi-bangla Abhidhan (Arabic-Bengali Dictionary). Dhaka: Islamic Foundation.

Karzon, Sheik Hafizur Rahman. (2008). Theoretical and Applied Criminology (1st edn.). (n.p.).

Lane, Edward William. (n.d.). Arabic English Lexicon.

Maik. (1980). Al-MuaÏÏÉ. DÉr IÍ yÉ' al-TurÉth Publishing.

Parker. (1980). Computer Abuse Research Update.

Qadri, S.M. Afzal. (2005). Criminology (5th edn.).

Quala'zi, Mohhamad. (2002). Fiqh OthmÉnÊ. Dhaka: Adhunik Prokashoni.

Siddiqi, Muhammad Iqbal. (1979), The Penal Law of Islam (1st edn.,). N.p.

Slater, Don. (2002). "Social Relationships and Identity Online and Offline", in L.Lievrouw and S.Livingston (edn.), The Handbook of New Media. London: Sage publications.

Subhas, P. Rathore and Bharat, B. Das. (2000). Cyber Crimes: The Emerging Trends and Challenges, Souvenir, national Conference on Cyber Laws and Legal Education NALSAR University of Law.

Sussman, Michael A. (1999). The Critical Challenges from the International High- Tech and computer-related Crime at the Millennium. FUKEJ. COMP & INLT L..

Watkins. (Janurary 1981). "Computer Crime: Separating the Myth from Reality", in C.A. Magazine.