Society & Change
Vol. VIII, No. 1, January-March 2014
ISSN :1997-1052 (Print), 227-202X (Online)

Combating Cybercrime in Bangladesh: National and International Legal Frameworks

Mohammad Mamunur Rashid*
Sharmin Akter**

Abstract

Technology driven crime, more generally known as Cybercrime[1] , has become grievous pus in the unceasing progression of science, technology and engineering. It is now a worldwide phenomenon as the scientists, engineers and law enforcing agencies are getting very serious regarding security and safety of mass use of technological equipment specially computer and internet. The patterns of committing cybercrimes are constantly changing. Hence, brunt of this heinous technological crime is also inconsiderably affected Bangladesh with its mass wave throughout the globe. Due to urgency of high cost of security enhancement protocol and legitimate software, developing countries like Bangladesh cannot enforce strict law regarding cybercrime and, investigation of cybercrime, collection of evidence for prosecuting cybercriminals require adept specialist with adequate training and budget. Moreover, preventing this sort of high-tech crime requires international cooperation with national initiatives. This article will argue that the cybercrime will not be prevented by only national initiative without cooperation from international arena even if the crime is committed in the computer located in Bangladesh. It will also argue that national law is more responsible to prevent this crime as the domestic law is capable to supersede the international laws. In doing so, it will try to suggest for accommodating harmonized, universally standard, and cooperative laws as well as policies considering the national and international politics with the diplomatic hands.

Key Words: Cybercrime in Bangladesh, Global effort, Legal, National Effort.

---

* Senior Lecturer, Faculty of Law, Eastern University, Bangladesh
** Lecturer, Faculty of Law, Eastern University, Bangladesh

[1] "Computer crime." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 20 June 2014 .Web. 3 Jul. 2014 . >http://en.wikipedia.org/wiki/Computer_crime>.

> "Human beings are vulnerable so rule of law is required to protect them [the human beings]'. Applying this [principle] to the cyberspace [,] we may say that computers are vulnerable so rule of law is required to protect and safeguard them [computer] against cybercrime."[2]

Introduction

Having entrusted with the fundamental traits of conventional crime, Technology driven crime, more generally, cybercrime[3] has achieved the status to be crime maintaining some differentiations from the traditional and theoretical definition of crime and criminal punishment. It is also committed by specific act or omission amounting into breach of rules and hence it is backed by sanction as well.[4] It was not long ago when the various activities i.e. Hacking, Circulating Viruses and so on were considered as merely fun. Now this is considered as great threat for the computer, technology and mostly security systems (of a country which almost reserve all information of security system in the computer or security system is regulated by the computer for its better protection). Moreover, it has been accelerating because of the expertise of the people who are operating the full matters keeping *mens rea*. In addition to these, this uniquely dangerous crime is committed by some professional or organized groups of criminals having equipped with enough expertise of cutting edge technology mostly for monetary benefits in an unauthorized way. Practically, computer crime possesses some unique challenges to the law enforcing agencies, investigators and prosecutors because the cyberspace[5] has no geographical boundaries. It can be done by computer criminals from anywhere of the world. Besides this, commission of this crime is possible anonymously hiding the identity of criminals in order to evade detective force. Recently the law enforcing agencies are trying to oversee the anonymous cyber criminals but they are facing unique technical and legal challenges to conduct their activities.[6] Because of the global nature of the cybercrime, determining the jurisdiction for prosecuting this crime is also big ramification. Considering the

---

[2] Haque, Aneek R., *Cyber Security in Bangladesh.* N.p., n.d. Web. 6 January, 2014. Visit for details: www.bdnog.org/v2/conference_paper/Cyber_Security.pdf.

[3] "Computer Crime." Wikipedia: The Free Encyclopedia, Wikimedia Foundation, Inc. visit for details: http://en.wikipedia.org/wiki/Computer_crime.

[4] Khalid, A. (n.d.). *Cyber Crime and Bangladesh Perspective* [online] Academia.edu, visit for details: http://www.academia.edu/4488760/Cyber_Crime_and_Bangladesh_Perspective Accessed on 16 January, 2014.

[5] "Cyberspace." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc.. http://en.wikipedia.org/wiki/Cyberspace.

[6] Aldesco, Albert I. "Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, The." *Loy. LA Ent. L. Rev.* 23 (2002): 81.

worldwide spread of this crime and challenges to control it, major international organizations, like the Organization for Economic Co-operation and Development (OECD) and the G-8 have been seriously discussing for cooperative schemes where many countries have not been showing the interest of combating this crime urgently for, *inter alia*, different approach of the different nation to piracy, espionage or social phenomenon. However, the objective of this article is to find out what roles should be played by Bangladesh to strengthen the initiative for preventing the cybercrimes. In doing so, it would try to show why Bangladesh might not be capable to control the cybercrime without cooperation of the international community.

Definition of Cybercrime: Is it misnomer?

Cybercrime[7]/computer crime is defined usually as a set of 'crimes' using the computerized data or software in major aspects. The definition of cybercrime is a complex, ever changing, and difficult but defining cybercrime is precondition for commencing investigation, prosecution, and above all raising awareness among the citizenry about the impact and worldwide dangers of this crime in order to assist the stakeholders. Surprisingly we cannot make any exhaustive definition of it irrespective of country, nation or place of occurrence.[8] The FBI (Federal Bureau of Investigation) defined cybercrime as cyber-terrorism which is pre-planned and politically motivated aggression against information, technology and computer system.[9] If we try to define cybercrime more broadly then we have to define it thus 'cybercrime is the illegal behavior committed by means of or in relation to a computer system or network by possessing, offering or distributing information by means of computer system or network.[10] Grabosky defined it, to some extent, similar to the conventional crime. He argued 'cybercrime is simply old wine in a new bottle'.[11]

---

[7] "Computer crime." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc, 20 January, 2014Visit for details: http://en.wikipedia.org/wiki/Computer_ crime.

[8] Siddiqui, M . S., *The Financial Express*, 2013., titled: 'ICT Act And Freedom Of Expression', 29 September, 2013, see for details: http://www.thefinancialexpress,bd.com/old/index.php?ref=MjBfMDlfMjlfMTNf MV85Ml8xODUxMDM=

[9] Janczewski, Lech, and Andrew M. Colarik, (eds.), *Cyber warfare and Cyber Terrorism*, IGI Global, 2008.

[10] "Cyber Crime In Contemporary World Information Technology Essay," UKessays.com. 11 2013, All Answers Ltd. 07 2014, See for details: http://www.ukessays.com/essays/information-technology/cyber-crime-in-contemporary-world-information technology- essay.php?cref=1.

[11] Grabosky, P.N., *Virtual criminality: Old wine in new bottles?, Social and Legal Studies*, (2001), (10:2), pp. 243-249:243.

Definition will be clearer if we consider the popular classification of cybercrime made by Goodman. These are:[12]

a. Crimes Where a Computer is the Target

In this case, computer of innocent individual might be intruded by criminal's computer as a target object of the cybercrime. Trespass, vandalism, sabotage, theft of intellectual property, extortion based on threats to release information stolen from a target's computer system, terrorist activities threatening for political purposes and so on might be example of this type of crime.

b. Crimes Where a Computer is a Tool of the Crime

Computer might be used as tool for committing crime. In this respect, actually crime is prevalent for the time immemorial, now computer is used as tool to commit those historical crimes. For instance, creation of counterfeit currency or official documents using computer scanners and graphics programs, embezzlement using a computer to skim very small sums of money from a large number of accounts, distribution of child pornography on the internet, theft of digital property and so on. Similarly fraud, hate crimes, stalking, gambling, and money laundering might also be committed through the internet where computer is used only as tool.

c. Crimes Where a Computer is Incidental

In this case, commission of crime does not require computer, it takes mere assistance from the computer for accomplishing any activity which is related to that cybercrime. For instance, the records of financial expenses and transaction of the drug dealer have been stored in the computer or inculpatory bomb recipe is discovered from the computer hard drive after explosion of its neighboring town.

Cybercrime simply relates to the damages or losses on the computer or technology not to society or the elements of the society, the human beings. From traditional perception it might appear to us as no crime at all. Practically the individual operating the computer or technology misuses it to lose on the other's computer and he has *mens rea* or *malafide* intention. The impact of this occurrence ultimately affects the society and human security in every aspect. Consequently it requires to be deemed as crime for protecting the human beings from digital catastrophe for warranting more civilized and enjoyable society. The traditional belief of existence of sanction for the crime is also present in case of cybercrime. As a result, cybercrime is crime, there is no misnomer.

---

[12] Goodman, Marc D. *"Why the police don't care about computer crime." Harv. JL & Tech.* 10 (1996): p. 465

History and Background of Cybercrime in Bangladesh

Computer and technology usage in Bangladesh is very recent and ipso facto, cybercrime has not been familiar in Bangladesh for the considerable time as it is unthinkable without emergence of Internet; internet usage has begun in Bangladesh since early 1990s. It has started its journey by commencing dialup access to e-mail using the Bulletin Board Systems (BBSs) for the first time when the number of users was not more than about 500. It conducted its business of internet service using the kilobyte for charging from the users and transfer of e-mail from one service provider to the rest of the world by international dialup; UUCP.

To accelerate the internet service, Government invited applications for subscribing the Very Small Aperture Terminal (VSAT).[13] On June 4, 1996 the VSAT connection was commissioned and the internet was launched in Bangladesh for the first time. Surprisingly, the first practical application of the internet in national arena was processing the publication of the National polls Result in 1996.[14]

Initially internet could not attract people due to the unavailability of the computer and scarcity of knowledge of the people regarding the utility of the internet and compute. It could also not draw the attention of the people as the price of computer was illogically high and unaffordable for them due to monopoly of the IPSs (internet service providers). It achieved the tremendous speed in increasing the users in 1997 as the number of ISPs increased; the amount of users and ISPs were approximately ten and twelve thousands respectively on that year. Later on, it developed and spread out more throughout the country for the various policies taken by the ISPs industries basically.

The government of Bangladesh has adopted more liberal national policies for a sustainable and rapid growth of the ISPs industry and as a result we had 180 ISPs by 2005.[15] In 2006, Bangladesh got connected with Submarine Cable (SEA-ME-WE 4 Submarine Cable) which afforded big bandwidth and low cost service than ever before.[16] After

---

[13] "Very-small-aperture terminal." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, see for details: http://en.wikipedia.org/wiki/Very-small-aperture_terminal>

[14] Hamidur Rashid, *Internet History of Bangladesh*, last visited 01.10.2009 <http://ezinearticles.com/?Internet-Histor of- Bangladesh&id=2327010.

[15] "Internet in Bangladesh." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 17 January, 2014 http://en.wikipedia.org/wiki/Internet_in_Bangladesh >

[16] Kamal, Mohammad Mostufa, et al, *Asian Social Science 8.15 (2012), titled:* "Nature of Cyber Crime and Its Impacts on Young People: A Case from

this, Bangladesh Telecommunications Company Ltd., BTCL (Now BTRC, 'Bangladesh Telecommunication Regulatory Commission') reduced the bandwidth price at regular intervals which attracted more and more users towards the internet world. As of now, BTRC has about three hundred and forty five (ISP Natiowide-94, ISP Central Zone-79, ISP Zonal-53, ISP Category A-99, ISP Category B-16, ISP Category C-04) registered ISP license holders and there are approximately 4.5 million users connected to them which is about 0.32% of our total population.[17]

The number of internet subscriber in Bangladesh grew from 186,000 in 2000 and to 617300 in 2009 successively. By 2011, the number of Internet users in Bangladesh had seen phenomenal growth of over 900% bringing the total number of users to 5,501,609 (3.5% of the total population) mainly due to wide availability of mobile Internet access. In 2013, Internet users in Bangladesh increased to 33 million. The Internet's speed in Bangladesh is not also among the fastest in the world but it has significantly developed in the recent past. As of April 2014, Bangladesh ranked 138th out of 190 countries on the Household Download Index by Net Index.[18]

This is the historical background of the computer and technology usage in Bangladesh. This unprecedented increase of the usage of computer and technology in the modern times posed the possibility of creating the way of various cybercrimes. This tendency has been well-founded on the basis of various recent examples. It is undoubtedly evident that Bangladesh has been deeply affected by cyber criminals. Attack in RAB's website in 2008 by a local hacker named Shahi Mirza was a major demonstration to the trepidation regarding accumulation of organized cybercriminals. Moreover, the felon confessed to police that not only RAB's website but also other national, government and nongovernment, and international site had been hacked by him for a long time. Totally he hacked 21 websites together with Army's website. So it is clear to us that the cyberspace of Bangladesh is not secured.[19] With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging

---

Bangladesh": p.171.

17 Summary of- BTRC licenses, Last visited 06.09.2009http://www.btrc.gov.bd/licensing/operators/summary_of_licenses.pdf

18 Ibid.

19 Hasan, Md Mehedi. *Nilakas-duronto.blogspot.hk*. N, titlted:'Nil Akas: Cyber Law And Its Weakness: Bangladesh Perspective'. .p. 2011,

legal issues relating to cyberspace, cyber law or the Law of internet came into existence in Bangladesh.[20] Information, Communication and Technology (ICT) Act 2006 was the first milestone towards peoples' concern regarding cybercrime in Bangladesh. Apart from ICT Act, Pornography Control Act 2012 and Copyright Act 2000 are some giant leap towards ameliorating cybercrime threat.

International Legal Frameworks Combating Cyber Threat:

Due to intricacy of cybercrime, the law and enforcing agencies are encountering daunting challenges to control the cybercrime. Hence, it requires the national and international cooperative initiatives to control it properly. Many countries are trying to accomplish under the shelter of many international organizations. We are discussing these first. Then we will concentrate our discussion to the national initiative of Bangladesh to protect the computer and technology from the attack of cybercrime.

In 1997, the Group of Eight (G8) established a "Subcommittee on High-Tech Crimes", dealing with the fight against cybercrime.[21]It adopted ten principles and ten action plan to fight against the cybercrime and destroy probable ways of committing this crime. It urges to maintain the cooperation between and among the member-states to regulate the full prosecution process even it from the investigation stage. It enlisted some crimes (child pornography, hacking and blocking websites, and so on) as major concern. It also settled a place of common communication for the member state to prosecute this crime.

The United Nations has undertaken several important approaches to address the challenges of cybercrime. It adopted resolution which addressed child pornography, anything done for child pornography significantly,[22] and it developed action oriented policy to prevent this crime.[23] It also invited the members to take step, law, policy,[24] maintain

---

[20] *"Weakness Of Cyber Law In Bangladesh Information Technology Essay." UKessays.com. 11 2013.*
See for details: http://www.ukessays.com/essays/information-technology/weakness-of-cyber-law-in-bangladesh-information-technology-essay.php?cref=1.

[21] Gercke, Marco, *"Understanding cybercrime: Phenomena, challenges and legal response," International TelecommunicationUnion (2012).*

[22] Article 2, 3 of the resolution of the UNGA 45/12, see for details: http://www.un.org/documents/ga/res/45/a45r121.htm, last visited on: 24th January, 2014.

[23] UNGA Resolution 45/121g v, see for details: http://www.un.org/documents/ga/res/45/a45r121.htm, laste visited: 24th January, 2014.

[24] UNGAA Resolution 56/12, see for details: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, last visited: 23rd January, 2014.

international cooperation to prevent this crime.[25] Moreover, it established Working Groups of the United Nations Counter-Terrorism Implementation Task Force (CTITF) on September, 2006 to accommodate the member states to pledge their cooperation to combat cybercrime in national and international arena. In this pledge, the CTITF formed the Global Counter-Terrorism Strategy which detailed the aims of this working group including the countering of financing toward terrorism.[26]

In 2011, the CTITF shifted their focus on the aim to "bring together stakeholders and partners on the issue of the abuse of the Internet for terrorist purposes, including through radicalization, recruitment, training, operational planning, fundraising and other means".[27] Under the UNODC, the NGO and Society for the Policing of Cyberspace (POLCYB) use international network to influence public and private organizational levels in aspects such as prevention, research and anti-corruption of cybercrime.[28]

International Telecommunication Union (ITU) works for modeling international policy on Global Cyber security Agenda and it thus promotes its main goals of using model legislation such as that of the Budapest Convention on Cybercrime for Member States and creating a Cyber Security Readiness Index.[29] The UN Economic and Social Council (ECOSOC) adopted resolutions, 2004/26[30] titled "International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Fraud, the Criminal Misuse and Falsification of Identity and Related Crimes." This resolution detailed the illegitimacy and classification of identity theft or fraud.[31]

The Council of Europe is playing an active role in addressing the challenges of cybercrime. The European Committee on Crime Problems

---

[25] UNGA Resolution 57/239 and 58/199, see for details: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf and last visited: 23rd January, 2014.

[26] Ki-moon,Ban., Berger, Maria., Costa, A. Maria and Orr , Robert (2007, May). , Advancing the Implementation of the United Nations Global Counter-Terrorism Strategy. Symposium conducted at the meeting of United Nations Office on Drugs and Crime, Vienna International Centre, Austria.

[27] Un.org, ''Working Group On Countering The Use Of The Internet For Terrorist Purposes - Counter-Terrorism Implementation Task Force'.

[28] Ibid.

[29] Butani, Anita, Bryan Chao, and Ninteenth Annual Session. *"Commission on crime prevention and criminal justice."* (2002): 9.

[30] Besides these it adopted 10, 149, 45, 50, 52, and 58 resolutions which have definitely addressed the IT issues.

[31] *edisonmun.files.wordpress.com/2011/05/cyber-terrorism.doc*

(CDPC) decided in 1996 to set up a committee of experts to deal with cyber crime.[32]It recommends the governments of member states to adopt the appropriate laws and policies for combating the cybercrimes.

Over the past decade, the European Union (EU) has developed several legal instruments addressing aspects of cybercrime. While those instruments are in general only binding for the 27 Member States, several countries and regions are using the EU standards as a reference point in their national and regional discussions on harmonization of legislation.[33] The EU Directive on Electronic Commerce addresses, among other issues, the liability of Internet Service Providers (ISPs) for acts committed by third parties. Taking into account the challenges stemming from the international dimension of the network, the drafters decided to develop legal standards to provide a framework for the overall development of the information society and to support overall economic development as well as the work of law-enforcing agencies. [34] In 2000, the Council of the European Union undertook an approach to address child pornography on the Internet.[35] It urges for the cooperation, constructive dialogue, and mutual communication among the member-states to fight against the cybercrime.[36] In 2001, the EU adopted the first legal framework directly addressing aspects of cybercrime.[37] It encourages government of member-state to take initiative to oblige the uses of the computer without deleting, altering the computer data and the attacking on the systems of the program.

In 2005, the Council adopted the EU Data Retention Directive. It contains an obligation for ISPs to store certain traffic data that are necessary for the identification of criminal offenders in cyberspace. [38] The first cybercrime-related draft legal framework presented after the ratification of the Treaty of Lisbon was the proposal for a Directive on

---

[32] Archick, Kristin. "*Cybercrime: The council of Europe convention." Congressional Research Service, Library of Congress,* 2005.

[33] Ibid.

[34] Id.

[35] Opinion of the Economic and Social Committee on the "Proposal for a Decision of the European Parliament and of the Council amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks" (COM(2002) 152 final — 2002/0071 (COD)) < http://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002AE1012>

[36] Article 2,3,4, and 5, of the

[37] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, Official Journal L 149 , 02/06/2001 P. 0001 – 0004 < http://eur-lex.europa.eu/legal- content/EN/TXT/?uri=CELEX:32001F0413>

[38] Ibid.

Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography 1200 that was adopted in 2011.[39] The Asia-Pacific Economic Cooperation (APEC)[40] has identified cybercrime as an important field of activity, and APEC leaders have called for closer cooperation among officials involved in the fight against cybercrime.

Taking into account the rising importance of cybercrime, the Law Ministers of the Commonwealth countries decided to order an expert group to develop a legal framework for combating cybercrime on the basis of the Council of Europe Convention on Cybercrime.[41] The Commonwealth Network of IT and Development (COMNET-IT) co-organized training on cybercrime in April 2007.[42] During the extra-ordinary conference of the African Union Ministers in charge of Communication and Information Technologies which was held in Johannesburg in 2009, the ministers of the member states addressed various topics related to the increasing use of ICT in the African country.[43] In 2011, the African Union presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. The Convention is more comprehensive than the most other regional approaches. It contains four parts. Part-one is related to electronic commerce. The second-part deals with data protection issues. The third part is related to combating cybercrime. The fourth part is dedicated to national cyber security monitoring structures.[44]

A number of countries in the Arabic region have already undertaken national measures and adopted approaches to combat cybercrime, or are in the process of drafting legislation. Examples of such countries include Pakistan, Egypt and the United Arabic Emirates (UAE). In order to harmonize legislation in the region, UAE submitted model legislation to the Arab League (Guiding Law to Fight IT Crime).[45]

The Organization of American States (OAS) has actively been addressing the issue of cybercrime since 1999 within the region. Among

---

39 Id.

40 Yamazawa, Ippei. *Asia Pacific economic cooperation*. Blackwell Publishing Ltd, 2011.

41 Chambers-Jones, Clare. "*Cyber economic crime and commonwealth laws." International Journal of Intellectual Property Management* 6.1 (2013): 95-110.

42 Gessi, Tania, Devindra Ramnarine, and John Wilkins, (eds.), *Asia Pacific Journal of Public Administration* 29.2 (2007): titled:"Introducing a New E-Governance Framework in the Commonwealth: From Theory to Practice." pp.131-151.

43 Ibid.

44 Orji, Uchenna Jerome, "*The defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity." Cybersecurity Summit (WCS), 2012 Third Worldwide*. IEEE, 2012.

45 Ibid.

others, the organization has held a number of meetings within the mandate and scope of REMJA, the Ministers of Justice or Ministers or Attorneys General of the Americas.[46]

ITU and the EU launched the project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR) in December 2008, to promote the ICT sector in the Caribbean region.[47] The project forms part of the program "ACP-Information and Communication Technologies" and the ninth European Development Fund. Beneficiary countries are Caribbean countries. The aim of the project is to assist CARIFORUM countries to harmonize their ICT policies and legal frameworks.[48] In parallel to the ITU and EU co-funded project in the Caribbean the same organizations launched a project in the Pacific (ICB4PAC).[49]

National Legislation Combating Cyber Threat:

There was no specific law regarding cybercrime or computer crime till 2006 in Bangladesh. Here was an endeavor to prosecute the high-tech criminals under the existing Penal Code, 1860 referring it as crime under that law. The Information, Communication and Technology Act, 2006, Pornography Control Act, 2012 and the Copyright Act, 2010 are special measure for preventing the special crimes; cybercrimes.[50]

Sections 54 and 57 of the ICT Act describe the cybercrimes from the civil and criminal perspectives.[51] In accordance with the ICT Act, 2006, a person damaging computer system of other,[52] tampering with computer source code,[53] hacking with computer system with illegal access,[54] publishing defaming, fake and obscene information in website,[55] being certified authority fails to surrender a certificate under section 34,[56]failing

---

46 Mugarura, Norman, *The Global AML Framework and its Jurisdictional Limits*, Diss. University of East London, 2012.

47 Lawton, Opal. "Monitoring Caribbean information societies", *LC/W* 315 (2010).

48 Girvan, Norman,*"Implications of the Cariforum-EC EPA," Caribbean Policy Development Centre* (2008).

49 Yoon, Chin Saik, "*Asia-Pacific ICTs: An overview of diversity" Digital Review of Asia Pacific' http://Asia-Pacific Development Information Programme of the United Nations Development Programme, http://Pan Asia Networking Programme of the International Development Research Centre, http://Orbicom, http://Southbound, http://www. digital-review. org/bhp01. htm* 1 (2006).

50 Ibid.

51 Id.

52 S. 54 of the Information, Communication and Technology Act, 2006.

53 S.55, ibid.

54 S. 56, id.

55 S. 57, id.

56 S. 58, id.

to comply with any order made under section 45,[57] failing to comply any order made under section 46,[58] securing access to any system violating section 47,[59] representing anything to controller of certifying authority to achieve the license of digital signature, or digital signature,[60] disclosing the confidentiality or privacy[61], punishing a false or fake digital signature,[62] making available any certificate, license, digital signature for fraudulent purposes,[63] assisting to commit these crimes[64] and being the director, secretary, partner. Shareholder or stuff of any company committing these crimes[65] would be considered as the criminals under this Act.

Pornography[66] is a crime and it is punishable when he is convicted for committing it without consent of the concerned individual. He may be penalized for seven years of imprisonment as per section 8 of the Pornography Control Act, 2012. Considering the expansion of the child pornography, this Act contains separate provisions for the child pornography and the imprisonment for this offense would be 10 years. Practically, the child pornography is created by the animation or artificial process. That is why it difficult to accuse any person for this crime.

Copyright[67] Act is a milestone to fight certain kind of cybercrime such as Piracy, Illegal distribution of media contents such as audios, videos and documents, theft of intellectual property etc.[68] The owner of copyright works has the exclusive right to do certain acts in respect of the work. If any person does any of these acts without having authority, s/he will be liable for the infringement of copyright.

[57] S. 59, id.
[58] S. 60, id.
[59] S. 61, id.
[60] S. 62, id.
[61] S. 63, id.
[62] S. 64, id.
[63] S. 65, id.
[64] S. 66, id.
[65] S. 67, id.
[66] Pornography is any dialogue, acting, posture, unclothed or partially unclothed dance in cinema, video, photography, graphics, audio-visual image or imagery otherwise captured and displayable, which causes sexual arousal and has no artistic or educative value. Also, such books, magazines, sculptures, cartoons and leaflets which cause the sexual arousal, and their negatives and so` copies would also be considered pornography.
[67] Section 71 of the Copyright in a work is deemed to be infringed when any person without a license from the owner of the copyright, or the Registrar of the copyright, or in contravention of the conditions of a license granted or any conditions imposed by a competent authority under Act
[68] Azam, M. (2006). Law and Our Rights. [online] Archive.thedailystar.net. Available at: khttp://archive.thedailystar.net/law/2006/02/01/education.htm [Accessed 16 Jan. 2014].

Combating the Cybercrime Bangladesh: National and International and Ramification

Actually it is not our target to comparatively discuss what superb and excellent laws are prevalent in Bangladesh and international arena to combat the cybercrime. Here, it is objective to find out what drawback or loopholes of these laws are creating impediments for having fruitful impact on preventing the cybercrime. We have already discussed what types of initiatives have been taken in both arenas. Now we would like to discuss what drawbacks are the main and fundamental culprits in the way forward.

Having the transnational nature,[69] the cooperation between the national and international community is predominantly required for preventing this modern and high-tech crime. Practically, it can be committed by anyone sitting anywhere of the world. At same time, if all countries of the world agree to prosecute the cybercriminals except one vested country, such heaven of the cybercriminals would destroy the whole technological achievement of the universe accommodating the criminals. Hence, adopting laws would be more fruitful and effective, if Bangladesh might create the environment to cooperate with other countries of the World. International law will not function superseding the national laws. That the procedure of the investigation and inquiry of the cybercrimes in national and international arena is not in harmony at all has been creating another problem.

Offenders can, in general, target users of any country of the world. As a result, offenders can be brought under surveillance if the cooperation among the states' law enforcing agencies can be bridged properly. Even the Investigation of the cybercrime requires means of cooperation and issues of the harmonization of concerned laws of the states.[70]

Practically national effort is more significant than the international effort. Unfortunately the national effort of many states including Bangladesh is not satisfactory in this respect. It may be more relevant when we will see that one example is cybercrime in our country but it is not crime in another country. Consequently, this crime should be

[69] Maruf, Ashiquddin Mohammad, Islam, Md. Rabiul Islam, and Ahamed, Bulbul (jointly authored), In: *Northern University Journal of Law* 1 (2014) titled: "Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies", pp.112-124.

[70] Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12 schjolberg.pdf.

prevented nationally. For instance, cyber gambling is offence in our country. It is not offence in USA. Again the impact of the cybercrime may also be different from country to country. For example, Spam-related e- mails especially affect developing countries. Due to scarcer and more limited resources, spam turns out to be a much more serious problem in developing countries than in western countries. The concerned affected country should take initiative. Here the developed and western countries might not come forward. Unfortunately, it is very much difficult for the developing country, if the offence s committed from the developed country. Consequently, the offenders will not be punished and the affected country might not create any diplomatic pressure on those countries to prevent the offenders.

National initiative may face a number of problems if it tries to take action denying the international cooperation or is obliged to take action. In regard to traditional crimes, the decision by one country, or a few countries, to criminalize certain behaviors of the offenders may be done very easily. In compare to this scenario, the action taken against the cybercriminals may not be as easily implemented as the criminals may stand anywhere of the world. In this situation, the court and the persons engaged with the justice system should think about the diplomatic relation between these states, the existence of the treaty of extradition, and specific statute of defining the cybercrime and so on. Section 4 of ICT Act 2006, tries to elucidate the gap by enumerating inter-state application of this Act stating that the person committing any crime contravening this Act outside of Bangladesh using the computer located inside or outside of Bangladesh shall be deemed as he commits crime under this Act.

It is true, ICT Act tries to take into consideration cross-border modern cybercrime, and this provision is not enough to adopt certain measures to combat with such crimes of transnational character. On the contrary, if the criminals act from a country that does not criminalize certain behavior, international investigations as well as extradition requests will very often fail. One of the key aims of international legal approaches is, therefore, to prevent the creation of such safe havens by providing and applying global standards. As a result, national initiative may require additional extra measures which have not been even properly pondered by Bangladesh yet.

We are crying for preventing the cybercrime to protect our security in national, personal and international level. Sometimes, when the government takes any step and it violates our simple personal interest then we take it so negatively that government cannot act properly in this

regard. For example, the freedom of speech is fundamental right. Newspapers are at liberty to express their opinion and critique against the faults of the government. Sometimes it crosses the limit. When government tries to control such unlimited liberty, we are apathy to that act thus the government should face the unexpected criticism. For example, the cabinet approved the draft of the ICT (Amendment) Act-2013 on August 19 proposing to empower law enforcers to arrest any person without warrant and increase the highest punishment to 14 years from minimum 7 years.[71] Punishment varies from seven years imprisonment to fourteen years imprisonment or fine may vary from five lakh (0.5 million) to 1 crore (10 million BDT) or both. After passing this law, Government has been encountering unexpected criticisms from the all sectors of the citizens.

Happy news is that cyber tribunal has been established. We are in doubt how much it will be successful to combat this crime as a session judge or an additional session judge is empowered to preside over the Cyber Tribunal. Ridiculously judges and lawyers are the experts of laws, not of technology, more specifically of internet technology. Similarly the investigation officers have no ABC knowledge on technology or internet activities. Hence, judges, investigation officers and the lawyers should be trained and made expert in technological knowledge for ensuring the justice of in technological disputes. Last but not the least; the mass people should be made aware about the cybercrimes and remedial procedures of this harassment.[72]

Conclusion:

To recapitulate, it can be said that cybercrime is the global and universal phenomenon and it has no exclusive territory to be committed. As a result, the measure of preventing it should not be taken in isolation by any country. For this purpose, we should determine a universal definition of cybercrime which would be applicable for any state irrespective of geographical location. In the same way, the laws and policies should also be harmonized for prosecuting the criminals.

No sovereign state the right to oblige any sovereign state to prosecute any criminal. Practically the criminals might not be the citizen of the affected country. As a result, the affected country should come forward to develop their laws and policies as well regulation to prosecute those

---

71 Siddiqui, M. S. (2013*), The financial express*,, tilted: 'New ICT law a threat to freedom of expression', available at http://www.thefinancialexpress-bd.com/old/index.php?ref=MjBfMDlfMjJfMTNfMV85Ml8xODQyNjE

72 Maruf, Ashiquddin Mohammad, Md Rabiul Islam, and Bulbul Ahamed (jointly), *Northern University Journal of Law* 1 (2014), tilted: "Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies.", pp. 112-124.

criminals. Here, the national law might get priority over the international laws. Interestingly, it may not function if the extradition treaty has not been already made between the countries. Cybercrime having the transboundary nature, all states should cooperate to combat this crime. If any state does not function for fighting against this crime, the criminals may attack on each and every computer and technological achievement of the universe from the country creating habitats for the criminals. As a result, this country should come under the regulation.

It is evident that preventing cybercrime requires bi-directional digging though the tunnels, each of the approaches has unique difficulties and advantages. Technology in today's world is one of the fastest changing things, so are the patterns, motives, ways of committing IT-related crime. It is unfortunate that Bangladesh has had little success in combating modern cybercrime though legislative measures. ICT Act and Pornography Act can prevent some of the banal cybercrimes that are almost obsolete, but a complete fiasco to the more ominous crimes such as money laundering, online theft, credit card hacking, virtual child pornography, and online fraudulence by image deformation, piracy and plagiarism, stock exchange fraudulence and so on. It has neither entered into a global pact regarding cybercrime nor strengthened existing laws nor updated according to the necessity nor applied them effectively. IT sector is growing pretty haphazardly which may backfire in near future which can be easily predicted by the recent aggravation of the situation. Cybercrime is like population explosion, once out of control, possesses an extremely daunting task to control. It is high time, Bangladesh should ponder upon this grievous threat and lessen the gap between international effort and national effort accordingly.

References

Haque, Aneek R., *Cyber Security in Bangladesh.* N.p., n.d., www.bdnog.org/v2/conference_paper/Cyber_Security.pdf.

"Computer Crime." visit for details: http://en.wikipedia.org/wiki/Computer_crime.

Khalid, A. (n.d.). *Cyber Crime and Bangladesh Perspective* [online] Academia.edu, http://www.academia.edu/4488760/Cyber_Crime_and_Bangladesh_Perspective

Siddiqui, M . S., *The Financial Express,* 2013, http://www.thefinancialexpress-bd.com/old/index.php?ref=MjBfMDlfMjlfMTNfMV85Ml8xODUxMDM=

Janczewski, Lech, and Andrew M. Colarik, (eds.), *Cyber warfare and Cyber Terrorism*, IGI Global, 2008.

Grabosky, P.N., *Virtual criminality: Old wine in new bottles?, Social and Legal Studies*, (2001), (10:2), pp. 243-249:243.

Goodman, Mar c D. *"Why the police don't car e about computer crime." Harv. JL & Tech.* 10 (1996): p. 465

"Very-small-apertureterminal,"http://en.wikipedia.org/wiki/Very-small-aperture_ terminal>

Hamidur Rashid, *Internet History of Bangladesh*, last visited 01.10.2009 <http://eziнearticles.com/?Internet-Histor of- Bangladesh&id=2327010.

"Internet in Bangladesh," http://en.wikipedia.org/wiki/Internet_in_Bangladesh >

Kamal, Mohammad Mostufa, et al, *Asian Social Science 8.15 (2012), titled:* "Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh*"*: p.171.

Summary of- BTRC licenses, http://www.btrc.gov.bd/licensing/operators/summary_ of_licenses.pdf

Hasan, Md Mehedi. *Nilakas-duronto.blogspot.hk*. N, titlted:'Nil Akas: Cyber Law And Its Weakness: Bangladesh Perspective'. .p. 2011,

Gercke, Marco, *"Understanding cybercrime: Phenomena, challenges and legal response," International TelecommunicationUnion (2012).*

Butani, Anita, Bryan Chao, and Nineteenth Annual Session, *"Commission on crime prevention and criminal justice."* (2002): 9.

edisonmun.files.wordpress.com/2011/05/cyber-terrorism.doc

Archick, Kristin. "*Cybercrime: The council of Europe convention." Congressional Research Service, Library of Congress,* 2005.

Gessi, Tania, Devindra Ramnarine, and John Wilkins, (eds.), *Asia Pacific Journal of Public Administration* 29.2 (2007): titled:"Introducing a New E-Governance Framework in the Commonwealth: From Theory to Practice." pp.131-151.

Orji, Uchenna Jerome, "*The defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity." Cybersecurity Summit (WCS), 2012 Third Worldwide*. IEEE, 2012.

Mugarura, Norman, *The Global AML Framework and its Jurisdictional Limits*, Diss. University of East London, 2012.

Azam, M. (2006). Law and Our Rights. [online] Archive.thedailystar.net. Available at: khttp://archive.thedailystar.net/law/2006/02/01/education.htm

Maruf, Ashiquddin Mohammad, Islam, Md. Rabiul Islam, and Ahamed, Bulbul , In: *Northern University Journal of Law* 1 (2014) titled: "Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies", pp.112-124.

Siddiqui, M. S. (2013*), The financial express,*, tilted: 'New ICT law a threat to freedom of expression': '', available at http://www.thefinancialexpress-bd.com/old/index.php?ref=MjBfMDlfMjJfMTNfMV85Ml8xODQyNjE

Maruf, Ashiquddin Mohammad, Md Rabiul Islam, and Bulbul Ahamed (jointly), *Northern University Journal of Law* 1 (2014), tilted: "Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies.", pp. 112-124.