



Major Threats of Cyber Crime in the Current Scenario: A Study on Bangladesh Perspective

Md. Shahidul Islam

Department of Law and Justice, Faculty of Science & Humanities, Bangladesh Army University of Engineering & Technology, Qadirabad Cantonment, Natore-6431, Bangladesh

Abstract: The present contemporary world is called the age of science & technology. People living in this world a borderless world that is known as cyber (Internet) world. In this world, internet has become a part & parcel of our daily life. People are now doing things easily by using information technology. The Internet is the technique of living to fulfill our needs. People are dependent on internet for various purposes such as communication, official activities, education and e-mail etc. In the present day, people are getting advantages from internet & misused for illegal activities. The main objective of this article is to know how the cyber crime is a threat to the technology and analyze the different provisions under ICT Act, 2006 for the prevention of cyber crime. Secondary sources have been used during the time of the research. However, this article has provided some recommendations such as; provisions relating to preventions of cyber crimes & role of the government and mechanism for creating public awareness to prevent cyber crimes.

Keywords: *Information Technology; Cyber Crime; Hacking; Police Power; Cyber Tribunal*

Introduction: As the present world is a cyber world, so the use of computer has been tremendously increased in everyday lives. People use computer, internet, smart cell phones which ensures better, faster, securer and more confidential service. It makes the whole world as a family & turns into a global world. Bangladesh is a developing country. There are a lot of scopes for development in Bangladesh by using information technology. In 21st century, Bangladesh has been developed on technology. The government is trying to progress more effectively to scattered internet at all levels of the country. People are totally dependent on internet & technology to meet up their livelihoods on various sectors. The people are gradually dependent on information technology and new crime; new threat to this technology has been up-and-coming. The technology possesses both useful side & harmful side. This is so because cyber crime turns into the undeviating way of such development. Cyber crime is that crime which is committed through networks (internet). This new-fangled crime is frequently increasing in Bangladesh. Cyber Crime is a global issue in the world. It is now a great danger to the technology in Bangladesh.

In order to take necessary action to prevent cyber crime strict laws are necessary. In the Information and Communication Technology Act, 2006 and ICT (Amendment) Act, 2013 there are several clauses relating to cyber crime but this Information and Communication Technology

Article history:

Received 26 April 2017

Received in revised form 7 June 2017

Accepted 10 June 2017

Available online 30 June 2017

Corresponding author details:

E-mail: bauetlaw@yahoo.com

Tel: +88 01712 536212

Copyright © 2017 BAUET, all rights reserved

Act is not exhaustive one to prevent cyber crime. Thus, considering these harmful facts a complete legislation should be introduced to tackle the possible danger of technology. This article aims to point out the major threat areas of cyber crime in the current scenario & recommends the mechanism to overcome the situation in Bangladesh. Opening part of this article discusses the statement of the problem, aims & objectives, materials & methodology and conception of cyber crime. Second part of the study focuses main causes of cyber crime threats & its kinds. After that the study emphasizes existing laws & its flaws with major cyber threat areas. Moreover, subsequent parts of the article focus its finding & recommendation to prevent cyber threat.

Statement of the Problem: During the preparation of this research article, it was found the following problems of cyber laws & cyber crimes in Bangladesh:

- (a) The jurisdiction of internet boundaries is unlimited. As a result the people may have easy access into the websites. For example, hacking to the website of an organization, govt. website etc.
- (b) People have easy access to the web sites that are available through internet, smart phones etc.
- (c) The internet users very often upload any despicable substance that may create an irritation surrounded by other net user. The materials which are vulnerable subjects similar to religious conviction, political affairs, child pornography and other detestable resources is considered a cyber crime in Bangladesh [1].
- (d) People may simply download illegal items (e.g., malware, viruses, pornography etc.) & documents (pictures, videos, etc.) of other person from the internet. They download these items due to their either lack of knowledge or to commit cyber crime. Thus, downloading & circulating illegal items from the internet becomes a great threat now- a- days.
- (e) Threat to modern technology has been increased through internet by using social communication (face book, imo, whatsapp, viber etc.) & it became a great danger to the national security of the country.
- (f) There are a few severe computer-generated crimes, for example distribution awful messages that are able to have an effect on set of computer connections and squash mailboxes.
- (g) By sending virus and spam mails all the way through internet is a cyber crime. This is because it can cause severe damage to the computer system.
- (h) When people copy from the software to CDs and DVDs that are copyrighted and spread of these materials on the internet is cyber crime & it is punishable offence Moreover, the ICT Act does not deal with any crime committed through using smart mobile phones.

Aims & Objectives of the Study: In the present contemporary world, the human activity depends on technologies used in almost all fields of people activity (such as communications, transport, space, power industry, water supplying, finances, trading, science, education, defense,

public maintenance of law and order, medicine, intellectual property and so on). After analyzing the various problems, statutes and its flaws of the ICT Act, the following most important objectives are found:

- i. To analyze & discuss hacking & mischief of computer and computer system and broadly discuss about the publication of fake, offensive and libelous announcement or in sequence in the internet in any way;
- ii. To deal with the matters anticipation, analysis, examination and penalty of cyber crimes and to develop mechanism for creating public awareness of cyber crime and cyber security challenges at all levels;
- iii. To discuss the areas of cyber crime which are under threat, related provisions under ICT Act, Govt policy & application of international instruments as well.

Materials & Methodology: This Paper is descriptive and suggestive in nature. It was based on documentary analysis and was not necessary to do wide fieldwork or scientific analysis. This paper was based on secondary data collected from Constitution of Bangladesh, ICT Act, 2006, Penal Code, 1860, The Evidence Act, 1872, The Code of Criminal Procedure, 1898, The Code of Civil procedure, 1908 etc. The material has been referred from book reviews, articles, journals, reports, text-books, newspaper, websites (Internet) etc. The collected data have been processed and prepared in the past form in order to make the study more useful, systematic and constructive for the users.

Conception of Cyber Crime and Definition: The term ‘cyber crime’ has been originated from two words ‘cyber’ and ‘crime’. ‘Crime’ is more or less known to each individual on his own stand point, while ‘cyber’ is almost vague in meaning to the same. Actually the issues which are related to internet (information technology) covers under the cyber grouping. In general sense, cyber crimes can be defined as ‘Crime against individual or organization by using of computer. The Information and Communication Technology Act, 2006 provides the offences which are cyber crime in Bangladesh as follows: if any person whoever:

- (a) Predicament of mainframe of computer and its system [2].
- (b) Modification of starting place code of computer [3].
- (c) Hacking in computer networks [4].
- (d) Publish any scandalous statement on the internet [5].
- (e) Entrance in put to one side of computer system [6].
- (f) Artificial electronic mark documentation [7].
- (g) Spread of confidentiality [8].
- (h) Reveal artificial sign for dishonest purpose [9].
- (i) Commend misdemeanor throughout internet [10].

The Penal Code, 1860 of Bangladesh states the crimes as the person who commits crime of the spiritual thoughts with ill motives of any group of the citizens in any way verbal abuse or endeavor to abuse the faith or the spiritual thoughts of that group, shall be punished [11].

The Constitution of Bangladesh provides [12]. that right of consideration and sense of right and wrong, right of words and thought, right of press of every citizen is guaranteed subject to restrictions. Thus, cyber crime means crimes in which a computer or its network is used to commit a crime as tool or become a target of a crime [13].

Causes for Cyber Crime: Cyber threats in the modern time of technology are slowly rising in different line of attack and it is sometimes unforeseeable. Any person may become the victims of this crime. An online newspaper reports that 73 percent women subject to cyber crime in Bangladesh [14].

The following are the major causes & reasons for the cyber crime and cyber vulnerability:

1. Illiteracy & lack of education: Due to the illiteracy of the net user, Bangladeshi people face some restrictions in right to use to information from the internet. As a result access & use to the internet is not easy to them. The major difficulties are the deficient of an incorporated computer safety measures system and edification. They don't have sufficient knowledge about the use of computer network system.
2. Private Information is online: If a person intentionally & unauthorized entrances, change, remove, break, demolish, or interrupt any computer, computer network, or computer program is considered a cyber trespass. In most cases it was found that the internet users keep their personal confidential data or information on online. As a result, cyber criminals are able to unauthorized access into the other accounts. For example, spam email, hacking a web page, breaking into a personal computer etc.
3. Comparatively small space of capacity to store data: The computer is a machine which has unique characteristic to accumulate internet materials into a very miniature breathing space. For example, RAM, ROM, Hard Disk, CD, pen drive, etc. As a consequence, people may very shortly eliminate or draw from information whichever from first to last objectively or subjectively [15].
4. Weak operating system & Carelessness: It is very closely connected with an individual performance. It is therefore found that the user after using the computer system, by negligence, left away the network (internet) open or not logout properly. Therefore, criminals easily split throughout into the network system. This is because computer operators have no adequate knowledge to operate any computer network properly.

5. Availability of internet through smart phones: Technology enhances human activities very short, comfortable & busy. Internet is now available in the all kinds of mobile phones. By using internet through mobile phones, the users may very often commit cyber crime without their ill motives.

6. Poverty & unemployment: It is for the most part of the primary grounds intended for consigning computer crime in Bangladesh. Due to poverty and joblessness, a person may search to earn money. When he has no money, no job, he commits cyber crime. For example, digital black mail. In this way, a cyber criminal may distribute & publish adding an exposed picture of another man & woman through internet and demand money from the victim(s).

7. Cyber criminals almost never get caught. The reasons behind this are- (a) cyber law is not in the same maturity as traditional law. For example, a hacker can attack you from anywhere in the world; (b) they operate internationally and it's very hard to track one down internationally. If you do track him/her down, it can be impossible to get the local police to corroborate; (c) needs very high level of technical expertise. For example, Hackers behind \$81 Million cyber heist – one of the world's biggest ever-from Bangladesh bank will never be caught as they are 'untraceable' and could go dark within minutes.

Kinds of Cyber Crime: In recent years, cyber crime is the widespread unpleasant incident in this modern world. The criminals may have connection with the criminals of another country by using information and communication technology. This technology can be used as a means of cyber crime. Therefore, it is evident that the computer, internet data may also be used in a caustic, anti-social mode, and so forth. The advance of ICT also gives the opportunity to the criminals to commit crimes. New types of cyber crimes such as hacking, cyber terrorism, cyber defamation, violates the right to privacy of a person, cyber pornography, data theft, denial of service attack, cyber frauds etc. are remarkable.

Hacking: Hacking has increased as a burning issue today's technological world. Hacking is arguably the most popular and well-known cyber crime. Hacking involves the unlawful access to another's computer without the legitimate owner's permission. By hacking a hacker access unauthorized use of another person's computer & may destroy or theft important data. Government websites of a country are the most targeted sites for the hackers. For example, the account of Barisal DC office was hacked in 2003 [16, 17] and Bangladesh Bank official's computer was hacked on February 2016.

Virus and worms attacks: It is a major problem that when a computer virus attack or access into another computer, it may delete data of that computer or stop the computer to run. These are diminutive software programs. It disperses very quickly as of one computer to another and to obstruct with workstation of computer operation system. A virus not only (a) Destroys, break, debase or harmfully have an effect on the performance of a computer resource but also (b)

connect itself to a new computer [18]. For example, PSW Bugbear, Lovegate. F, Trile. C, Mapson etc.

Computer & ATM Fraud: It is one kind of expected fraud for individual accomplish by the exercise of computer network systems. This is because PIN numbers of ATM card are often missing or forgotten by the users. In case of Bangladesh, 11 people supposedly caught up in ATM card counterfeit by duplicating cards. Bangladesh's influential force Rapid Action Battalion (RAB) made the arrests from Dhaka [19]. Case study 2- ATM frauds were also happened in Bangladesh Bank, three commercial banks (Eastern Bank Ltd, United Commercial Bank Ltd and the City Bank. Police investigated the captured video footage of four ATM booths & found that at least Tk 25 lakh were made theft [20].

Cyber Pornography: Cyber pornography covers pornographic websites, pornographic magazines, child pornography, films, images, text video which describes or show sexual acts etc. ICT Act, 2006 clearly ensures the punishment with maximum 14 years imprisonment & fine up to tk. one crore for publishing or spreading pornographical activities throughout the internet [21].

Cyber Terrorism: The word 'cyber terrorism' has two elements: cyberspace and terrorism. In this way the cyber criminals firstly plan & then attack on user's computer & network systems.

Cyber Defamation: It is one of the significant cyber crimes now in Bangladesh. By cyber defamation the VIP & high status persons are harassed. As a result, the reputations of general people are under threat. According to Penal Code, 1860 provides the elements of defamation such as by words, spoken, sign, written, recording, email, sms, and caricature, effigy either temporary or permanent in nature by electronic form provided it must be defamatory & published to third parties [22].

For example, 'P' drew a picture of A, B and C that shows that they were doing homosexual activities. Subsequently P tagged this picture to his face book wall and shared it to his others face book fans or sent this picture through email to his friend W. The drawing and publication of such picture is called cyber defamation and it is punishable offence under section 57 of Information & and Communication Technology Act, 2006. The daily Prothom -Alo shows that most of the cases are filed for defamation under section 57 of the Information Communication Technology (Amendment) Act, 2013 [23]. However, recent statistics from the cyber tribunal shows that this law is being used to harass people with baseless cases. Therefore, many news cases were filed & under investigation after the establishment of cyber tribunal. In most of cases under section 57 were filed for posting offensive pictures or videos of women on Face book. Spiritual values, making distasteful remarks about VIPs, and publishing indecent news throughout internet are noteworthy.

Privacy violation & Identity Theft: The Constitution of Bangladesh ensures fundamental rights of every citizen to privacy of his correspondence and other means of communication [24]. Sometimes people keep their personal data such as email addresses, phone number and account details on social media etc. Hackers get the advantage from these sites by stealing or hacking personal information. These cyber crimes are dangerous in nature and always create serious threat to privacy at personal, public or national level. For example, in 2012 the Ramu Sadism case in Cox's Bazar [25]. Someone open with a fake Face book account & upload a photo of desecration of the Holy Quran on its wall. The fake account was under a Buddhist male name. This post apprehensive the general Muslim people of that area and they, without verifying the authenticity of the Face book account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were damaged. So, it is clear that Bangladesh is not free from the threat of cyber-crimes. Everyday new forms of cyber-crimes are happening and if it goes unchecked, law and order situation will deteriorate.

Electronic funds transfer & money laundering: Most of the banks are providing services through online banking, stock exchange transactions but are not able to provide the highest security. In Bangladesh's financial institutions especially banks are at risk from hackers. The cyber criminal through internet may have an opportunity to attack country's technology communications. Moreover, software pirated & copy right infringement, trademark and service mark violation, theft of computer source code, computer vandalism means deliberately destroying or damaging property of another, E-mail spoofing are remarkable cyber crimes. As a result, our business sector is now on threat.

Cyber Laws in Bangladesh: There are very few laws regarding cyber crime in Bangladesh. The Information & Communication Act, 2006 is one of them. In this law section 56(1) & 57 has declared the penalty of 14 years imprisonment with or without fine. Section 68 of the said Act has declared the formation of a special tribunal named "Cyber Tribunal". Moreover, the establishment of Cyber Tribunal in the district court the Session Judge has the power to take cognizance to trial such kind of crime under. In Bangladesh, BTRC which perform as a supervisory body to prevent cyber protection. It has the power to accomplish mobile courts. The Constitution of Bangladesh ensures protection of home & correspondence as a fundamental right as well as human right under article 43. Moreover, Cyber security Act, 2015 and Digital Security Act, 2016 has already been drafted in Bangladesh to prevent cyber crime. Some important cyber crimes in Bangladesh are mentioned as follows: Hacking, Virus dissemination, Software piracy, Pornography, Credit card fraud, Defamation, E-mail spoofing, posing statements etc are crucial. Consequently, economy, medical sector, business center, public & private offices, education system, individuals, group of individuals, communications, intellectual property, security of the state etc. are under threat.

Findings & Recommendations: The foregoing discussions expose various deficiency and complication regarding the threat of cyber crime in Bangladesh. The following discussion

summarizes the deficiencies and complication of cyber crime and put forward the suggestions to prevent cyber crime in Bangladesh. Major findings and suggestions are given below:

1. Cyber crimes are rising everyday and it turn out to be a great deal on the way to check and reprimand. Therefore, a check and balance must be adopted by the govt to introduce some standard policy between police power of arrest without warrant and citizen's protection against arbitrary arrest and detention guaranteed in article 33 of the Constitution.

2. Arbitrary arrest may be increased by the amendment of ICT Act, 2013 because of by this amendment police may arrest a person without warrant. There is scope of misuse this power. A victim's support center needed to be set up and fair & impartial justice must be ensured for them. The victims may report to the BTRC help line or ICT Division regarding suspicious online activities etc.

3. Due to digital laboratory investigation process are hampered and it becomes impracticable to provide evidence in support of the case. So, a digital laboratory has to be set up & well trained man power should be appointed to investigate & detect the cyber crime. For the protection & prevention of cyber crime, cyber crime legislation & Govt policy, Statutes, Rules etc. must be developed

4. In Bangladesh certain types of crime such as political, religious, or social speech, either explicitly or through vague wording are found. As a result, many innocent people are arrested, charged & imprisoned under ICT Act, 2006 for their posts on social networks regarding this.

5. Due to the shortage of the establishment of cyber Tribunal, it cannot provide satisfactory justice for the victims of cyber crimes. Moreover, the people should not keep their personal data on the internet and should not disclose any information to unknown persons by e-mail, sms or otherwise through social networks. By keeping social security numbers, account numbers, and passwords private, as well as specific information about users, such as user's full name and date of birth, it may be possible to prevent cyber crime.

6. The Law enforcement agency particularly police are not well trained to investigate such crimes and collect evidence. As a result, it is difficult to find and arrest real criminals. Law enforcement agency must abide by the directions given by Supreme Court in *BLAST vs. Bangladesh* [26] as to arrest. Police should exercise this power more effectively, consciously, on reasonable ground. They should not be biased politically & exercised power capriciously. A separate skilled cyber police unit may be introduced to identify cyber criminal.

7. Due to the shortage of well trained manpower in the special branch named "Anti-cyber Crime Department" it is very difficult to protect cyber crime and fulfill the main objectives of ICT Act. In this regard, public awareness can be increased for the using of internet. Government, Mass

Media, IT institutions should take awareness raising programmes so that people can understand that writing undesirable contents on the internet is an offence and it is punishable.

8. According to section 76(2), the offences of the ICT Act, 2006 are non-cognizable in nature. Moreover, there is no dedicated expertise and skilled trial lawyer and judges to dispose of cyber crime cases in the established cyber tribunal. This is the most important shortcoming of the Act. Thus, strict statutory laws needed to be passed by the Legislatures keeping in mind the interest of citizens. As cyber crime is a major threat worldwide, so to get rid of cyber crime, effective international policy is needed at the international level.

9. Procedural complexities and lack of proper executing system is another crisis of cyber crime. There should be a different policy for different internet users. The web site owners should adopt new policy for preventing cyber crimes. Not only this but also creating strong passwords with ten characters or more than that may be used to prevent cyber crime and needs anti-virus software to protect virus attacks.

10. Many financial institutions such as bank, company, insurance company, educational institutions, and other govt. & non-government organizations are in apprehension of commission of cyber crime. Thus, economically these institutions turn into backward sections of the competitive world and financially looser. Not only this but also a negative impression will arise about the business sector as a whole. Consequently, the business sectors may be fall down as a whole.

Conclusion: Internet is definitely the most essential technology of the modern-day world. The practical functions of technology make our life easier in every sector such as education, business, service, technology, entertainment etc. In Bangladesh, the major threat of the internet is the cyber security threat in recent years. Therefore, ICT Act, 2006 is comparatively more effective to combat cyber crime & penalize criminals. The Penal Code, 1860 was not enough to fulfill the needs of new crimes emerging from internet. Due to enormous development of information technology, new crimes are arising in different ways and means. Therefore, new strict legislation is needed to prevent those crimes in iron hand. Certain provisions of the Penal Code, 1860 and the Evidence Act, 1872 need to be amended in order to meet the new requirements of the cyber space crimes. To keep & maintain international peace and security, it is essential to promote & protect cyber laws. Bangladesh can also take necessary steps to prevent cyber crimes from the cyber space. The government in power is estimated to invest millions of taka to build a digital Bangladesh. So, the issue of cyber security should be given more priority & the govt. should come forward for taking necessary steps.

Acknowledgement: I am extremely grateful to my respected teacher Professor Dr. Sarkar Ali Akkas, Professor Dr. M. Ahsan Kabir and Professor Dr. M. Hashibul Alam Prodhan for their suggestion. This study may be carried out at Masters Level.

References:

- [1] Badsha Mia, Cyber Crime & its Impact in Bangladesh: A Quest for necessary Legislation, Law Mantra, (International Monthly Journal, ISSN 2321 6417), Volume 2, Issue 5, (2015).
- [2] Section 54 of Information and Communication Technology Act, 2006.
- [3] Section 55 of Information and Communication Technology Act, 2006.
- [4] Section 56 of Information and Communication Technology Act, 2006.
- [5] Section 57 of Information and Communication Technology Act, 2006.
- [6] Section 61 of Information and Communication Technology Act, 2006.
- [7] Section 63 of Information and Communication Technology Act, 2006.
- [8] Section 64 of Information and Communication Technology Act, 2006.
- [9] Section 65 of Information and Communication Technology Act, 2006.
- [10] Section 66 of Information and Communication Technology Act, 2006.
- [11] Section 295A, the Penal Code, 1860.
- [12] Article 39 of the Constitution of the People's Republic of Bangladesh.
- [13] Karnika Seth., J. Altamas Kabir, Computer, Internet, New Technology Laws, First ed., India-Islamic Culture Center, New Delhi, India, 2013.
- [14] Bdnews24.com, 9 March 2017.
- [15] Hart, The Concept of Law, <https://sites.google.com/site/cybercrimezbd/reasons-for-cyber-crime>, accessed on March 2017.
- [16,17] The Daily Star, Sunday, July 13, 2003 also cited Ashiquddin Mohammad Maruf, Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies, The Northern University Journal of Law, V.ISSN 2218-2578, 2010.
- [18] Section 54 (iii) of Information and Communication Technology (ICT) Act, 2006.
- [19] http://news.xinhuanet.com/english/2017-03/15/c_136131914.htm, accessed on May 2017.
- [20] <http://www.thedailystar.net/frontpage/foreigners-atm-fraud-ring-511822>, on February 16, 2016.
- [21] Section 57 of Information and Communication Technology Act, 2006
- [22] Section 499 of the Penal Code, 1860.
- [23] The daily Prothom-Alo, 24 September, 2016.
- [24] Article 43 of the Constitution of the People's Republic of Bangladesh.
- [25] <http://bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era.html>, August 12, 2015.
- [26] 55 DLR (2003) 363.