BAUET JOURNAL
Published by
Bangladesh Army University of Engineering & Technology
Journal Homepage: http://journal.bauet.ac.bd

MAJOR THREATS OF CYBER CRIME IN THE CURRENT SCENARIO: A STUDY ON BANGLADESG PERSPECTIVE

Md. Shahidul Islam
[1]*Law and Justice, Faculty of Science & Humanities, Bangladesh Army University of Engineering & Technology, 6431, Qadirabad Cantonment, Natore, 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. Nowadays, information technology makes tasks easier for people. Our method of l ife to meet our wants is the Internet. For many things, including communication, official tasks, education, and e-mail, people rely on the internet. People are currently taking advantage of the internet and abusing it for illicit purposes. Understanding how cybercrime poses a threat to technology and examining the various laws under the ICT Act of 2006 for cybercrime prevention are the primary goals of this essay. While conducting the research, secondary sources were consulted. Nonetheless, this article has offered some suggestions, including clauses on the government's role in preventing cybercrimes, measures to raise public knowledge of these issues, and other ideas awareness to prevent cyber crimes.

Keywords: *Information Technology, Cyber Crime, Hacking, Police Power, Cyber Tribunal.*

1. Introduction
As the present world is a cyber world, so the use of computer has been tremendously increased in everyday lives. People use smart phones, computers, and the internet to ensure better, faster, more secure, and more private services. It turns the entire planet into a global family. Bangladesh is a developing nation. Information technology has numerous opportunities for development in Bangladesh. Bangladesh has advanced technologically in the twenty-first century. At every level of the nation, the government is attempting to move more efficiently towards dispersed internet. People rely entirely on the internet and technology to support themselves in a variety of industries. The population is becoming more and more reliant on information technology, and new crimes are emerging that pose a threat to this technology. Both positive and negative aspects of the technology exist. This is the case because cybercrime becomes the unintended path of such growth. Crimes conducted through networks (the internet) are referred to as cybercrimes. Bangladesh is seeing a regular rise in this new type of crime. Cybercrime is a worldwide problem. It now poses a serious threat to Bangladeshi technology. Strict legislation is required in order to take the required steps to prevent cybercrime. In the Information

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 address: bauetlaw@yahoo.com
Telephone Number:+ 88 01712 536212

Although the Information and Communication Technology Act of 2006 and the ICT (Amendment) Act of 2013 contain a number of provisions pertaining to cybercrime, they are not all-inclusive in their efforts to prevent it. Therefore, a comprehensive law should be created to address the potential threat of technology in light of these detrimental facts. This article suggests a way to address the situation in Bangladesh and highlights the main areas of cybercrime danger in the current environment. The issue statement, goals and objectives, resources and technique, and the idea of cybercrime are all covered in the first section of this article. The key causes of cybercrime threats and their types are the subject of the study's second section. The report then highlights current legislation and its shortcomings in relation to key cyberthreat categories. The article's conclusions and suggestions for preventing cyber threats are also the main subject of the following sections.

1.1. Statement of the Problem

While preparing this research piece, the following issues with Bangladesh's cyber laws and cybercrimes were discovered:
(a) Internet limits have infinite jurisdiction. People may therefore find it simple to access the websites. For instance, breaking into a company's, government's, or other website.

(b) Websites that are accessible via the internet, smartphones, etc., are simple for people to use.

(c) Internet users frequently post anything vile that could irritate other computer users. In Bangladesh, cybercrime is defined as the use of materials including child pornography, political issues, religious convictions, and other reprehensible content that are susceptible to attack [1].

(d) People can easily download someone else's papers (photos, films, etc.) and illicit products (malware, viruses, pornography, etc.) via the internet. Either they are ignorant or they are committing cybercrime by downloading these products. Therefore, downloading and disseminating illicit content via the internet has become a serious risk in recent years.

(e) The use of social media platforms like Facebook, Instagram, WhatsApp, Viber, and others has escalated the threat to modern technology and put the nation's security at serious risk.

(f) Some serious offences involving computers include sending offensive messages that can affect a group of computer connections and smash mailboxes.
(g) Sending spam emails and viruses over the internet is considered a cybercrime. This is due to the possibility that it could seriously harm the computer system.

(h) It is considered cybercrime and a serious offence when individuals distribute copyrighted software on CDs and DVDs online. Additionally, the ICT Act does not address any offences involving the use of smartphones.

1.2. 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.

1.3. 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.

1.4. 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].

2. 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.

2.1. 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.

2.2. 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.

2.3 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.

2.4. 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].

2.5. 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].

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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.

3. Cyber Laws in Bangladesh

4. Regarding cybercrime, Bangladesh has very few laws. A 2006 law is the Information & Communication Act. This statute stipulates a 14-year prison sentence, with or without a fine, in sections 56(1) and 57. A unique tribunal called the "Cyber Tribunal" has been established, as stated in Section 68 of the aforementioned Act. Furthermore, a Cyber Tribunal has been established in the district court, and the Session Judge has the authority to take cognisance to try such a crime. The BTRC in Bangladesh serves as a regulatory organisation to stop cyberattacks. It has the ability to create mobile courts. Under article 43 of the Bangladeshi Constitution, the right to a home and correspondence is guaranteed as a fundamental human right. In order to combat cybercrime, Bangladesh has previously draughted the Cybersecurity Act of 2015 and the Digital Security Act of 2016. The following are a few significant cybercrimes in Bangladesh: spoofing emails, spreading viruses, software piracy, pornography, credit card fraud, defamation, and making false statements, among others. This puts the economy, the medical field, the business sector, public and private offices, the education system, individuals and groups of individuals, communications, intellectual property, state security, etc. at risk.

5. 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 raising 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 programmers 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.

6. Conclusion

The most important technology in the modern world is unquestionably the internet. Every aspect of our lives, including business, education, entertainment, and services, is made easier by the useful features of technology. In recent years, cyber security has become the biggest internet concern in Bangladesh. Therefore, in terms of fighting cybercrime and punishing offenders, the ICT Act of 2006 is relatively more effective. The Penal Code of 1860 was insufficient to address the demands of newly emerging online offences. New crimes are emerging through various techniques as a result of the tremendous advancements in information technology. Therefore, in order to stop those crimes in their tracks, new, stringent laws are required. The Evidence Act of 1872 and the Penal Code of 1860 both require amendments to satisfy the new standards for cyberspace offences. The promotion and protection of cyber laws is crucial to preserving and upholding global peace and security. The appropriate actions can also be taken by Bangladesh to stop cybercrimes from occurring online. The ruling government is thought to spend millions of

to create a digital Bangladesh. Therefore, cyber security should be prioritised and the government should take the required action.

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.1 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.