



Daffodil
International
University

Research on

**A Critical Overhaul of the Laws and their Trend Regulating the Cyber-crime in
Bangladesh**

Submitted By

Mohsin Uddin Showrov.

ID- (183-38-288)

Department of Law, Daffodil International University

Supervised By

Md. Abu Saleh

Assistant Professor

Department of Law

Daffodil International University

This research work is dedicated
To
My Beloved Parents
Md. Mozammel Haque and Monowara Begum

DECLARATION

I am completely alert that I have a pledged to clarify to the appraiser which is my own work, and which is made by others whom I am alluding to in my paper. Except if, I unmistakably ascertain something else, my appraiser is qualified for expect that everything being exhibited in the paper starts from me. More ever I proclaim that that I have not presented this paper or any bit of it, for assessment in any of my post-graduate coursework or other insightful endeavors. I am completely aware and mindful that reestablishing to written falsification which would lead me to get a characteristic of 'zero' and open me to facilitate disciplinary activities as recommended by the University's principles and controls.

Md. Mohshin Uddin

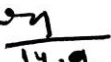
L.L.M

ID: 183-38-288

Department of Law, Daffodil International University

CERTIFICATION

This is to certify that the thesis on “A Critical Overhaul of the Laws and their Trend Regulating the Cyber-crime in Bangladesh” is done by Md. Mohshin Uddin Showrov in the partial satisfaction of the requirement for the degree of LL.M. from Daffodil International University of Bangladesh. The thesis has been carried out successfully under my guidance.

MAS 
14.9.2017

Md. Abu Saleh

Advisor

Assistant professor

Department of law

Daffodil International University

ACKNOWLEDGEMENT

First of all, I offer millions of heartfelt gratitude to my Almighty ALLAH, who, who has given me strength and his mercies and grace to finish of my Research Monograph successfully.

I feel very proud to express my heart-felt gratitude and appreciation to my honorable research supervisor Abu Saleh, Assistant Professor of department of law of Daffodil International University for his guidance, untiring interest, constructive criticism and creative suggestion throughout my research. It was his dedication and guidance during the study period that has greatly inspired me to prepare this Research Monograph successfully.

I would like to thank my other friends for their friendship. It helped me with mental support to go through this study. They also helped with the advice of using more advice technology made my work easily.

LIST OF ABBREVIATIONS

<u>Abbreviations</u>	<u>Title</u>
ACH	Automated Clearing House
DoS	Denial of Service
CID	Crime Investigation Department
HTTP	Hypertext Transfer Protocol
EFT	Electronic Funds Transfer
HCD	High Court Division
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technology
IGP	Inspector General of Police
IO	Investigation Officer
NGO	Non-Governmental Organization
NSA	National Security Agency
PCA	Pornography Control Act
UN	United Nations
USB	Universal Serial Bus
BTTB	Bangladesh Telegraph and Telephone Board
DEA	Drug Enforcement Agency
BSF	Border Security Forces
UNCTAD	United Nations Conference on Trade and Development

TABLE OF CONTENTS

<u>CHAPTER I</u>		
INTRODUCTION		
S.L.	Content	Page No.
1.1	Background of the study	1-2
1.2	Description and statement of Problem	2-3
1.3	Objectives of the Study	3
1.4	Methodology of the Study	3-4
1.5	Limitations of the study	4
1.6	Research Question	4
1.7	Brief literature review	5
1.8	Conclusion	5
<u>CHAPTER II</u>		
DEVELOPMENT AND PROGRESS OF CYBERCRIME		
2.1	Introduction	6
2.2	Definition of Cybercrime	6-7
2.3	Brief History of Cybercrime	7
2.4	Brief History of Cybercrime in Bangladesh	7-10
2.5	Classification of Cybercrime	10-11
2.6	Conclusion	11-12
<u>CHAPTER III</u>		
REASONS OF CYBERCRIME IN BANGLADESH AND ITS RECENT TREND		
3.1	Introduction	13
3.2	Reasons behind the cyber-crime in Bangladesh	13-14
3.3	Cyber-crime Committed in Bangladesh	14-16

3.4	Real scenario of cybercrime in Bangladesh	16
3.5	Case studies and the increasing of crimes	16-18
3.6	Conclusion	18
<u>CHAPTER IV</u>		
LEGAL PROTECTION AGAINST THE CYBER-CRIME IN BANGLADESH		
4.1	Introduction	19
4.2	Legislation in Bangladesh to control the Cybercrime	19-20
4.2.1	Information and Communication Technology Act, 2006	20-23
4.2.2	The Penal Code, 1860	23
4.2.3	The Pornography Control Act, 2012	23-24
4.2.4	Digital Security Act, 2018	24-26
<u>CHAPTER V</u>		
FINDING OF PROBLEMS OF THE STUDY		
5.1	Introduction	27
5.2	Finding problems	27-29
<u>CHAPTER VI</u>		
RECOMMENDATION		
6.1	Recommendations	30-31
<u>CHAPTER VII</u>		
CONCLUSION		
7.1	Conclusion	32
7.2	Selected Bibliography	33-34

CHAPTER 1

INTRODUCTION

1.1. BACKGROUND

We know that the present age is the technological age. The world is highly changing day by day. So, the modes of crime are also changing now. In Bangladesh, Cyber and technology related crimes are gradually increasing. At present, Cyber-crime becomes the most serious issue in Bangladesh. Already it has been seen that cyber-crime is a despondent warning which may become visible in the area of information and communication technology. In addition, we also saw that Cyber blustering is becoming a major anxiety for parents because of their children using the internet as their part of the subject by which majority of students in Bangladesh have experienced being disturbed online or being disturbed by the same person both their online or offline. Therefore, cyber-crimes are also becoming a warning to the government itself. In our country, there are only few laws to regulating and controlling the cyber-crime but this is not enough to control this type of crimes. Because of absence of legitimate enactment to control the cyber- crimes, most of the time cyber criminals are safe side after committing such crime. There are several clauses to control the cyber-crime which deals in the Information and Communication Technology Act-2006 and ICT (Amendment) Act-2013. But, this Act isn't concrete and enough against the cyber-crime. So, considering the above facts, there should be introduced and imposed a magnificent and comprehensive Cybercrime Protection Act. This research work incorporates overhaul of the laws of Bangladesh regulating the issues of Cyber-crime in Bangladesh.

In addition to that, if there have sufficient sources of information to the computer criminals to access the computer systems, then it has a possibility to commit a crime on that computer system. So, Cyber-crime may be an “unlawful act wherein the computer is either a tool or target or both”.¹ Bangladesh is now fixed its goal to become digital Bangladesh by vision 2021 with some specific goal by using of e-governance in all sectors of government agencies². There is no

¹ Sheikh Hafizur Rahman Karzon (2008)-Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, 411-418

² The initiative of nagorik committee,(2006), Bangladesh Vision 2021, August 2007, CPD, Available at Goal 2.3, <http://saber.eaber.org/sites/default/files/documents/Bangladesh%20Vision%202021.pdf> (Accessed: 20 September 2018)

doubt that Cybercrime crime become a global impact in short but it highly big history globally.³ So, in recent time, the nature and dimension of the cyber-crime has dramatically changed in Bangladesh. Therefore, it became necessary to identify the recent trend and issues of Cybercrime that why it is increasingly in Bangladesh and how to control and reduced this type of crimes.

1.2. Description and statement of Problem

Though Bangladesh is being classifications an underdeveloped nation however Bangladesh has seen a technological revolution gradually. Now, any adolescents of Bangladeshi can access to any PCs and different device effectively. Consequently, the hackers can get enough opportunity to take part in hacking and committing crimes. It has already been proven that hacking has become a serious problem in Bangladesh. It isn't just basically to the youngsters; however the perceived media is likewise typically occupied with the hacking and distributing private data.⁴

On 15/02/2012, there was an alleged that group of Bangladeshi hackers has been hacked in excess of 25000 Indian sites which included significant sites, for example, the site of the Border Security Forces (BSF). The name of the hackers was 'Black Hat Hackers'⁵. Moreover, we can specify the 2012 Ramu Violence in Cox's Bazaar where a horde of furious Muslims has been assaulted Buddhist hallowed places and a home, burning some of them Sunday in Bangladesh to dissent after a photograph of a somewhat consumed Quran was posted on face-book⁶. In this case, the attacks were totally pre-planned and co-ordinate. Along these lines, it is demonstrated that Bangladesh still isn't free from the danger of Cyber-crimes.

The most important and serious issue has been committed in recent times which all are knew. On March 11, 2016, \$101 million of Bangladesh Bank (BB) was taken and \$81 million was wired to two banks in the Philippines, but the remainder of \$20 million was sent to a bank in Sri

³ Badsha Mia, Cybercrime And Its Impact In Bangladesh: A Quest For Necessary Legislation,7

⁴ Md. Sarwar Alam Sajid, Cyber Crime and Legal Fabric of Bangladesh,12 August 2015, Available at <http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>(Accessed: 20 September 2018)

⁵ By Indo-Asian News Service, Bangladeshis hack 20000 Indian websites,5 June 2012, Available at <http://gadgets.ndtv.com/internet/news/bangladeshis-hack-20000-indian-websites-224516> (Accessed: 20 September 2018)

⁶ Farid Ahmed, Bangladesh Muslims torch Buddhist shrines: police say,1 October 2012, CNN, Available at <https://edition.cnn.com/2012/09/30/world/asia/bangladesh-muslim-buddhist-violence/>(Accessed: 20 September 2018)

Lanka for a NGO. This record was opened only a month back, as per the Bangladesh Bank.⁷ The modes and nature of cyber-crimes is changing now in Bangladesh. Therefore, it needs to be finding out and identified so that new mechanisms should be introduced to maintain the future law and order situations.

1.3. Objectives of the Study

The point and goals of my research is to analyzing, finding and concentrate in all forms of crimes persisting in the society and causes of this particular crime. Following objectives will be carried out in the study...

- a. To study the progress and development of cybercrime;
- b. To prevent the crime
- c. To study and dealing with the causes of cybercrime;
- d. To find and examines the cyber issues of Bangladesh;
- e. To protect youth generations and society,
- f. To identify the area this area still not explore by research
- g. To examine the legal protection in relating to the cybercrime;
- h. To study and discuss the forms of cybercrime;
- i. To discuss the interference strategies that will help to finish cybercrime.
- j. To promote the public awareness by encouraging to control the cyber-crime. In my research, the study will review and analyze the secondary literature, law and practices of Bangladesh in accordance with the methodology of the study and the relevant data.

1.4. Methodology of the Study

The methodology of my research paper is basically the qualitative (analytical) but in some special circumstances; I followed the quantitative measures (empirical). In carrying out the paper, I depended on the primary and secondary sources. The article is mostly literary based with a mixture of analytical reasoning .In my research; the secondary information will be gathered from

⁷ Rejaul Karim Byron and Md Fazlur Rahman, Hackers bugged BB system in Jan, 11 march 2016, The Daily Star, Available at <http://www.thedailystar.net/frontpage/hackers-bugged-bb-system-jan-789511>(Accessed: 20 September 2018)

the writing on the theme, Annual Reports of major non-legislative associations. In addition, data of my research will be gathered from the site of some national and international organizations. In my research I tried to evaluate all things. In the case of evaluation I have been given a few propositions by way of method for proposals which will be made in the finish of every chapter. But, an overall conclusion will be given in the last part of my examination.

1.5. Limitations of the study

Being required to complete the report timely, I faced the following limitations. Despite all these limitations, I have given the best of my efforts and tried to make the report as informative and comprehensive as possible. The study has been made basically based on secondary data and primary data and materials by both national and international institutions and individual studies. It might be noticed that the study of my research will for the most part center on women, child or juvenile victims. I also will focus on offenders if there is any special and important issue. We know that the word cyber-crime is progressively confined to clarifying the crime in which essentially utilized the PC or system which is a fundamental part of the cyber-crimes. This term is likewise in some cases utilized in the field of traditional crimes which are fraud, theft, blackmail etc. which mainly used the computer or network. Hence, as the utilization of computer has increment, so cyber-crime has turned out to be progressively significant and major issue. To control the cyber-crime - the existing laws alone are not enough. Therefore, it is important to control such type of crimes- the existing laws should be amended.

1.6. Research Question

As a researcher, I have some research question on which based I will complete my research. The research questions are as following....

1. Whether Bangladesh has sufficient law to control the cyber-crime?
2. What are the reasons behind the increasing of a cyber-crime in Bangladesh?
3. What is the legal procedure for controlling the cyber-crime?

1.7. Brief literature review

The world is changing day by day. The nature and modes of crime is also changing now. Since Cybercrime is a fast growing matter of discussion and research today's, there are more books and articles are written on my research topic. Therefore, on the legal relationship some other books which deal much significance. There is an Unseen or invisible Threat of Cyber-Terrorism by Dan Verton, Theoretical and Applied Criminology by Sheikh Hafizur Rahman Karzon, Criminology (Cybercrime) by Monjur Kader and Constitutional Law of Bangladesh by Mahmudul Islam. In addition to the above, a list of other books, articles, documents, statutes, and journals on a different view of Cyber issue may be found. The effort will be made in my research work to suggest reform where needed and update the existing laws so that an effective and efficient enforcing mechanism is ensured in a fruitful way to controlling the cyber issue.

1.8. CONCLUSION

Cybercrime is obviously the new dimension form of the crimes at present in the world which is very tough to suppress. But, it will not be difficult to prevent us to take adequate measures for controlling against the cyber-criminals. It is high time to control and prevent the upcoming cyber threats of Bangladesh and other related issues. By the proper and effective measures of the government and rising the awareness among the people- cyber-crime s can be reduced and control. The ordinary people ought to likewise be cautious in utilizing computer frameworks and online offices.

CHAPTER 2

DEVELOPMENT OF CYBERCRIME

2.1. INTRODUCTION

Though Bangladesh is being classifications an underdeveloped nation however Bangladesh has seen a technological revolution gradually. Now, any adolescents of Bangladeshi can access to any PCs and different device effectively. Consequently, the hackers can get enough opportunity to take part in hacking and committing crimes. It has already been proven that hacking has become a serious problem in Bangladesh. It isn't just basically to the youngsters; however the perceived media is likewise typically occupied with the hacking and distributing private data.⁸

2.2. DEFINITION OF CRIME

Now, we know about the term of cyber-crimes. A large portion of the individuals of our own realize this is a crime which carried out on the web. With the changing of the innovation cyber-crime is spreading everywhere throughout the world like a virus. During the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were created inside a related workshop around then.⁹ In a tight sense-Cyber-crime or computer crime is a crime of any unlawful conduct which utilized by methods for electronic act that center the security of PC frameworks and the information handled by utilizing them.

In a more extensive sense - Cyber-crime or PC related violations bargains any illicit conduct which perpetrated by methods for or in connection to a PC framework or system which including this sort of violations as unlawful belonging and offering or conveying data by methods for a PC framework or system.¹⁰

⁸ Md. Sarwar Alam Sajid, Cyber Crime and Legal Fabric of Bangladesh, 12 August 2015, Available at <http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/> (Accessed: 20 September 2018)

⁹ 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf

¹⁰ Kumar, Cyber Law, A view to social security, 2009, page 29

Generally, cyber-crime is the crime which is finished by utilizing PCs and the web. In other words, cyber-crime incorporates anything from downloading by any unlawful music records to taking a huge number of dollars from online financial balances.¹¹

There is a typical definition which portrays that cyber-crime as any action where focus on a PCs or systems or a position of crime.¹² A few definitions has been attempted to consider targets or expectations and characterize cyber-crime all the more exactly, for example, that PC interceded exercises which are either unlawful or considered illegal by specific gatherings and which can be led through worldwide electronic systems.¹³ The different approached and the related problems which refers that there are significant challenges in characterizing the terms of computer crime and cyber-crimes.¹⁴

2.3. Brief History of Cybercrime

At present-Cyber-crime is one of the biggest and comprehensively most risky issues of crime. All things considered, the web is now accessible and visible to everybody and that is the reason it includes dangers. Perpetrating a crime by means of a computer or other instrument that is connected with the Internet is risky on the grounds that the character of the offender is so hard to discover. It is accepted that the cyber-crime first recorded and occurred in 1820. The true fact that the computer existed since 3500BC in India, China and Japan however the modern computer started in 1937 with the logical motor of Charles Babbage.¹⁵ Despite the fact that the first known infection for a computer has been attracted up to 1980 but the people of the world truly didn't know until the Melissa infection began to assaults the a great many computer in late March 1999 in which the New Jersey State Police and the Federal Bureau of Investigation (FBI) embroiled the criminal .¹⁶ In the most punctual occasions roughly in 1970s that data security was applied to business computer systems then it was focus on the prevention of fraud.¹⁷

2.4. Brief History of Cyber-crime in Bangladesh

¹¹ Monjur Kader, theory and practice of criminology Bangladesh perspective, 2015, page 246

¹² Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin

¹³ Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3

¹⁴ Brenner, Cybercrime Metrics: Old Wine, New Bottles Virginia Journal of Law and Technology, Vol. 9, 2004

¹⁵ B.Magalla, the New Era of Cyberspace: Their Protection, Prevention and Detection. Tumaini University Iringa University College, 2013

¹⁶ S.Ghosh, and E. Turrini. A Multidisciplinary Analysis. Springer Verlag Berlin Heidelberg, 2010

¹⁷ Ibid

Though Bangladesh is being classifications an underdeveloped nation however Bangladesh has seen a technological revolution gradually. In 1995, the Secret Service and Drug Enforcement Agency (DEA) accomplished the main Internet wiretap which is usually similar to a telephone wiretap. The DEA had the option to close an organization who was selling phone by an illicit nature of cloning hardware.¹⁸ Its deceitful exercises are named as cyber-crime, e-crime, hi-tech crime, or electronic crime. These practices include the utilization of computer or web as a medium, source, instrument, target, or spot of a crime. These unlawful practices contain the utilization of computer or web as a medium, source, instrument, target, or spot of a crime. At present Computer and Internet assumes an imperative job in various kind of exercises which resembles recording financial transactions, steering phone calls, estimating power use, observing restorative medications, and so forth. With the improvement of information technology the field of cyber-crimes has expanded and the new arrangement of crimes have been imagined. However, it also contributed to electronic crimes which are as follows----

1. **Cyber Stalking:** the Oxford dictionary characterizes the stalking as a seeking after stealthily. Thus, Cyber Stalking includes following each move of a person over web by posting message. It might be finished with the assistance of numerous sources which accessible, for example, email, chat rooms, and client net gatherings, constantly bombarding the victims with the emails etc.
2. **Phishing:** phishing is like to fishing in a lake but instead of trying to capture fish. It is a procedure of pulling out private information from the bank/monetary institutional record holders by illicit nature or fake methods. In this case, the phishers try to steal our personal information.
3. **Hacking:** Hacking is a simple term which means unlawful trespass into a computer framework without the consent of proprietor or client and the person who hacks anything is called hacker. There was a reality that a functioning programmers bunch which driven by one Dr. Nuker, who guarantee to be author of Pakistan Hacker Club and apparently hacked the sites of Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nation, India.¹⁹

¹⁸ Ahmed, Dr. Zulfiqar, Cyber Law in Bangladesh, National Law Book Company, Dhaka, 2012, pp-221-265

¹⁹ Kader, Monjur, Criminology (Cybercrime), University press, Dhaka, 2008, pp-125-129

4. **Harassment via E-mails:** harassment via e-mails is not a new matter. It resembles to annoying by letters. As of late there was guarantee by the case of a woman wherein she complained about the harassment. Her previous boy friend was sending her mails persistently genuinely coerces to her and he likewise risk to her.²⁰
5. **E-mail Spoofing:** a spoofed e-mail can be said that it ought to be distorts to individuals its beginning by messages. Recently in India a spoofed e-mail were sent on the name of Mr. Vijayshamkar which essentially contained infection.²¹ However, e-mail spoofing that mail seems to begin from one source but really has been sent from another source.
6. **Cyber Defamation:** it is a demonstration of ascribing any individual with aim to bring down the individual society esteems or open the person to hatred, contempt. This is happen when defamation happens with the assistance of computer or potentially the web. For instance that if somebody distributes defamatory issue about somebody on a site or sends messages which containing the slanderous data or information, then it will be treated as cyber defamation.
7. **Computer vandalism:** generally- Vandalism implies purposely devastating or harming property of another. So computer vandalism may contain any sort of physical damage done to the computer of any individual. These demonstrations may appear as the robbery of a computer Vandalism.
8. **Intellectual property crimes / Distribution of pirated software:** literally -Intellectual property comprises of a bundle of rights. Any unlawful demonstration by which the proprietor is denied completely or mostly of his privileges is structured as an offense. The regular type of IPR infringement might be said to be programming robbery, copyright encroachment, trademark and administration mark infringement, burglary of computer source code, and so forth.
9. **Cyber pornography:** pornography entertainment on the web which may take different structures. It tends to be contained the facilitating of site which primarily containing the denied data. Digital sex or cyber pornography entertainment shows to depiction of sexual material on the web. Criminals regularly rape or attack a young lady and catch the

²⁰ Monjur Kader, theory and practice of criminology Bangladesh perspective, 2015, 252

²¹ Ibid.

episode by webcam or cell phone and afterward spread the video over internet. These events are getting to be alarming in the provincial territories of Bangladesh.

2.5. Classification of cyber-crimes

In my study, the term cybercrime incorporates digital war, cyber reconnaissance, cyber activism and cyber terrorism. The cybercrime can be classified into four classes which as pursues:
Cybercrime against individuals in persons:-

There are various types of cyber-crime against individuals which are-

- harassment via e-mails,
- cyber-stalking,
- defamation,
- Unauthorized control/access over computer system (hacking),
- indecent exposure,
- email spoofing,
- Cheating & fraud.²²

1. Cybercrime against individual property:

There are some different crimes which can be committed against individual's property.

Those are as follows—

- Credit card extortion,
- computer vandalism,
- transmitting pernicious code(virus/worm/Trojans),
- unauthorized control/access over computer framework (hacking),
- Intellectual property crimes which contains programming theft: unlawful replicating of projects, dispersion of duplicates of programming, copyright encroachment, trademarks infringement,
- theft of computer source code), and

²² E.H. Dalla, and M. Geeta. "Cyber Crime a Threat to Persons, Property, Government and Societies" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, No.5, pp.997-1002, 2013. Y. Joshi, and A. Singh, "A Study on Cyber Crime and Security Scenario in India "International Journal of Engineering and Management Research, Vol.3. No.3, pp.13-18, June 2013,

D. L. Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing, Inc, 2002

- Net trespass.²³

2. Cybercrime against organization:-

Sometimes cyber-crime is committed against government, various kinds of organizations firms, Companies and group of individuals. The cyber-crime against organization is as follows—

- denial of administration,
- email shelling,
- logic bomb,
- Trojans horse,
- data diddling,
- unauthorized control/access over PC framework,
- possession of unapproved data,
- Distribution of pilfered programming and cyber terrorism against the administration, organization and so on.²⁴

3. Cybercrime against society at large:

The crimes committed against societies mostly affect of our people mainly to against the young generation. This types of crimes are highly affect and harmful for the societies. The crimes against societies which are described in the following heads....

- pornography (fundamentally youngster pornography),
- polluting the young through disgusting introduction,
- trafficking,
- financial violations,
- Online betting or gambling,
- forgery and
- Web jacking.²⁵

2.6. CONCLUSION:

²³ Ibid

²⁴ Ibid

²⁵ Ibid

In spite of the fact that, Internet and web advances are becoming so quick in the present world but they are giving new chances and they are likewise comprising of specific dangers like-email undercover work, MasterCard extortion, spam's, programming theft etc. therefore should be careful about it.

CHAPTER 3

REASONS OF CYBERCRIME IN BANGLADESH AND ITS RECENT TREND

3.1.INTRODUCTION:

Generally, Computer crime or cybercrime is a type of crime where the person commits a crime by using the Internet or computers. The person who uses the online and access to the Internet, individual data in their computer, then they normally conveys significant information into the internet that can be attracted by the computer criminals.²⁶ Any kinds of criminal activity can be comes within the field of cybercrime that uses a computer either by an instrumentality, target or by some other methods for forever further crimes. We can see over the most recent couple of years, numerous states have made the most of the opportunity by ICT inside an arrangement structure which set out certain rules and continued with the definition of a national ICT system as a piece of the general national advancement plan. Presently Bangladesh has planned to utilize ICT as the principle significant component for financial improvement.

3.2 Reasons behind the cyber-crime in Bangladesh

There are a few explanations behind cyber-crime which are given below---

1. Easy to access –

The issue behind protection of a computer framework from unapproved access is that there are numerous chances of breach because of the overwhelming innovation. Since the Hackers can without much of a stretch access to our framework and he can take access codes, retina pictures, propelled voice recorders and so forth which can trick biometric frameworks effectively and sidestep firewalls can be used to move beyond numerous security frameworks.

1. Complexity of taking legal steps-

²⁶ Yar, M. (2005).The novelty of cybercrime an assessment in light of routine activity theory: European Society of Criminology, 2, 407-427

The complexity of taking legal steps against cyber criminals is one of the main causes behind expanding cyber-crime.

2. Negligence:-

Another reason behind the cyber-crime is the Negligence. Negligence is firmly associated with human conduct. It is probable that if there is any negligence for protecting the computer system, then there is possibility to the cyber-criminal to obtain entrance and authority over the computer framework effectively.

3. Another cause of cyber is that the criminals are expertise in technology.
4. There is less risk even no risk in such types of crimes. That's why the cyber related crimes are increasing.
5. The use of computer and other technology is spreading out in our societies. That's why the cyber related crimes are increasing.
6. Criminal law does not define the cyber-crime s properly. As a result cyber related crimes are increasing in our societies.
7. Invention of new techniques for crimes and the weakness of law enforcing agencies.
8. As the opportunities of traditional crimes are reducing so cyber-crime s are increasing.²⁷

Besides above described the causes of cyber-crime there are some different reasons for cyber-crimes which are as per the following...

1. **Economically Motivated cyber-crimes.** We know that today, numerous crimes are carried out outside the web; money is a central helper for many cyber criminals. This is a result of the perils of criminality which are less clear when we are holding up behind a system, the acknowledgment of okay and exceptionally high budgetary reward prompts numerous cyber criminals to participate in various sort's malware, phishing, data fraud and false cash solicitation assaults.
2. **Personally Motivated Cyber-crime:** Personally motivated is also another reasons for cyber-crime in our country. We realize that digital offenders are as yet people and what they do including their crimes are regularly the reason for individual feelings and family struggle. For this reasons, he introduces an infection on office PCs to an envious

²⁷ Monjur Kader, theory and practice of criminology Bangladesh perspective, 2015, page 249

sweetheart hacking into a lady friends web-based social networking accounts just to demonstrate that he could do it.

3.3 Cyber-crime Committed in Bangladesh

As Bangladesh is developing day by day and the technological knowledge is expanding, so cyber-crime is also expanding in our country. The first cyber-crimes started in Bangladesh with spam mails and Trojan attacks. Most of the cyber-crimes that are committed in Bangladesh are as follows.....

1. **Hacking:** Hacking is a basic term which means illicit trespass into a computer framework without the authorization of proprietor or client and the individual and the person who hacks anything is called hacker. Now-a-days, the hackers are much smarter than our thoughts. Few days ago, the hacker hacking of the website of the National Parliament of Bangladesh and keep their obscene pictures.
2. **Pornography:** Pornography on the web may take different structures. It tends to be contained the facilitating of site which essentially containing the prohibited information. Digital sex entertainment shows to depiction of sexual material on the web. Hoodlums frequently assault or attack a young lady and catch the occurrence by webcam or cell phone and after that spread the video over web. These events are getting to be disturbing in the country zones of Bangladesh.
3. **Cyber defamation:** It is a demonstration of attributing any individual with expectation to bring down the individual society values or expose the person to hatred, contempt. This is happen when criticism happens with the assistance of PCs as well as the web. For instance on the off chance that somebody distributes abusive issue about somebody on a site or sends messages which containing the slanderous data, then it will be treated as cyber defamation.
4. **Harassment via E-mails:** harassment through messages is certainly not another issue. It resembles to harassing by letters. Recently there was a claim by the claim of a woman wherein she complained about the harassment. Her previous boy friend was sending her mails continuously sincerely extorts to her and he additionally risk to her.²⁸

²⁸Monjur Kader, theory and practice of criminology Bangladesh perspective, 2015, page 252

5. **Denial of service attack:** A denial-of-service (DoS) is any sort of assault where the assailants (programmers) attempt to keep genuine clients from getting to the service. SO, Denial-of-service attacks in which malicious actors take actions to make systems, services and networks unusable can be carried out by flooding with them.²⁹
6. **Threatening:** Recently a threat was made to our honorable Prime Minister.
7. Virus dissemination
8. Software piracy
9. Credit card fraud
10. Net extortion

3.4 Real scenario of cybercrime in Bangladesh

As Bangladesh is developing day by day and the technological knowledge is expanding, so cyber-crime is also expanding in our country. The first cyber-crime s started in Bangladesh with spam mails and Trojan attacks. Our life is about a combination of good and malevolence. Along these lines, is the web, for all the great it said to us, Cyber space has its dull sides as well. There are no police officers to keep guard the data superhighway, leaving it opens to everything from Trojan ponies and infections to cyber stalking; trademark duplicating cyber terrorism.

3.5 Case studies and the increasing of crimes

Case1. On August 23, 2004, an email message was sent to Bengali daily Prothom Alo which giving an actual life threat to Awami League president and our honorable Prime Minister sheik Hasina. On August 25, 2004 Another mail was sent to the police central command which additionally containing the existence danger of former Prime Minister Khaleda Zia, her child Tarique Rahman and Bangladesh Nationalist Party (BNP) administrators. For this situation, the police division paid attention to the sends and chose to build up a cyber-crime control unit which unit will be the nation's initially policing unit against cyber-crime. In this issue, two youngsters, a private university student and a software engineer, have been captured in connection with the email undermining the Prime Minister Sheik Hasina and another adolescent for compromising the former Prime Minister Khaleda Zia.³⁰

²⁹ Techopedia, Available at <https://www.techopedia.com/definition/24841/denial-of-service-attack-dos> (Accessed 20 September 2019)

³⁰ Daily Prothomalo_23 August, 2004

Case 2. In 2008, there was a case that a pretty programmer of Bangladesh whose name was Shahee Mirza who hacked the RAB's website. He confessed to police that he had been hacking RAB's website as well as other national govt., non govt. and international sites for a long time. 21 sites had been hacked by him together with Army's site. In this way, for this situation, it is obvious to us that the internet of Bangladesh isn't still secured³¹ because there is no nationwide computer infrastructure, or security framework has yet been created in Bangladesh. For these reasons, the cyber-crime is expanding.

Case 3. On 15/02/2012, there was an incident a terrible event where it is alleged that a group of Bangladeshi programmers named Black Hat Hackers who hacked in excess of 25000 Indian sites which contained significant sites, for example, the site of the Border Security Forces (BSF). We see that the purposeful publicity exercises are additionally treated as cyber-crimes in certain examples. In this way, promulgation is data which is one-sided and misdirecting in nature mainly used to advance or expose a specific political reason. It makes complications and frenzy among the general people.

Case 4. We may describe the Ramu Violence in Cox's Bazar which has been occurred in 2012. In this case, an unknown person with a fake Face-book record posted a photograph of contamination of the Holy Quran on its divider. The phony or fake record was distributed with the name of a Buddhist male name. This post attacked the common Muslim individuals of that region however they are not checking the legitimacy of the Face-book record and they assaulted guiltless Buddhist inhabitants of that zone. Numerous Buddhist temples, religious communities and family units were destroyed.³² In this case, the attacks were totally pre-planned and coordinate. Thus, it is demonstrated that Bangladesh still isn't free from the risk of Cybercrimes.

Case 5. Recently, a terrible event has been occurred in February 2016 which is that the taking of \$101 million from the stores of the Bangladesh Bank has brought up an issue on the introduction of money related to cyber-crime group. This horrible occurrence has tested the capacity of existing instruments in preventing such episodes. But, this robbery meant the requirement for strengthening the worldwide participation in controlling the cyber-crime. The programmer's

³¹Hasan, Mahdy, Cyber-crime: Implementation and Must to Achieve Vision 2021, 30 June 2012, The Daily Star, Page 6

³²Om Farid Ahmed, Bangladesh Muslims torch Buddhist shrines: police say, 1 October 2012, CNN, <https://edition.cnn.com/2012/09/30/world/asia/bangladesh-muslim-buddhist-violence/>

recovered the national bank's exchange codes and sent installment move demands worth \$1 billion to the Federal Reserve Bank of New York. They mentioned the assets of Bangladesh moved the assets to a bank in the Philippines. From that point, the money was moved to at least three Philipino gambling clubs: At the club, somebody changed over the money into chips for wagering and after that reconverted the chips into money. After that the cash was then sent to financial balances in Hong Kong. An extra store of about US\$ 21 million was likewise moved illicitly to an outsider in Sri Lanka.³³

3.6 CONCLUSION:

Cybercrime is obviously the new dimension form of the crimes at present in the world which is very tough to suppress. But, it will not be difficult to prevent us to take adequate measures for controlling against the cyber-criminals. It is high time to control and prevent the upcoming cyber threats of Bangladesh and other related issues. By the proper and effective measures of the government and rising the awareness among the people- cyber-crime s can be reduced and control. The general people should to be cautious in utilizing computer frameworks and online offices. The nation ought to take all conceivable measure to prevent any sort of digital intrusion which may place the lives of individuals in a difficult situation. The general individuals ought to likewise be cautious while utilizing the PC frameworks and online offices. So we trust that our mindfulness and consistent protest against cyber-crime will bring about progress.

³³ Victor Mallet and Avantika Chilkoti, How cyber criminals targeted almost \$1bn in Bangladesh Bank heist, 18 March 2016, Financial Times, <https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8>

CHAPTER 4

LEGAL PROTECTION AGAINST THE CYBER-CRIME IN BANGLADESH

4.1. INTRODUCTION:

In Bangladesh, there are a few laws to deal with the cybercrime issues which, for example, The Information and Communication Technology (ICT) Act 2006, the Penal Code 1860, the Pornography Control Act (PCA) 2012. Recently, the government of Bangladesh has been passed a law which is the Digital Security Act, 2018. Among them three laws are very important for practical purposes which are -the ICT Act 2006, the PCA 2012 and the Digital Security Act, 2018. ³⁴Cyber pornography can be indicted by section 8 of the PCA. The digital stalking acts will be conceivable to keep on being resistant from legitimate procedure as these laws don't clearly characterize them and our preliminary judges will probably be unwilling to convict an individual for acts not characterized as crimes. The characteristic of the ICT Act 2006, it deals with the both purpose, substantive as well as procedural.

4.2. Legislation in Bangladesh to control the Cybercrime

At present-Cybercrime is one of the biggest and internationally most dangerous issues of crimes. All things considered, the internet is currently accessible to everyone and that is the reason it includes dangers. So, the modes of crime are also changing now. Information Technology has been brought by computers, computer systems, web and the internet. It additionally has been made numerous new issues in law on the grounds that; there was an inadequacy of enactment while managing the data innovation. Now, throughout the world -the judiciary dealing with the new problem like cybercrime, adjudication and investigation of cybercrime, intellectual property Rights issues in cyber world etc. In Bangladesh, Cyber and innovation related crime is progressively expanding. Presently, Cyber-crime is the genuine and noteworthy issue in Bangladesh. Hence, the most significant enactment of the Bangladesh Information and Communication Technology Act, 2006 and Information and Communication Technology

³⁴ Quazi MH Supan, CYBER CRIMES: Are women the main target, 10 March 2015, the daily star, <https://www.thedailystar.net/law-our-rights/cyber-crimes-70592>

(Amendment) Act, 2013 has been authorized (Sec. 4 of the ICT Act, 2006) to manage the matter of digital crimes . However, the Cybercrime may include crimes which are conventional in nature. This might be as robbery, extortion, fabrication, defamation and mischief, which are part to penal laws of our nation. For instance, Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 characterizes certain offense which doesn't cover by the Penal Code. That is the reason, it might be said that the Penal Code, 1860 isn't successful enough in managing cybercrimes in Bangladesh.

4.2.1 Information and Communication Technology Act, 2006:

In 2006, the parliament of Bangladesh has instituted the Information and Communication Technology Act, 2006 which characterizes and indicated specific kinds of exercises as crimes. The exercises will be the cybercrimes for the domain of Bangladesh, which has made punishable under the Information and Technology Act of 2006. The following table demonstrates the cybercrime and also their punishment.³⁵

Section	Name of Crime	Punishment
54	Mischief of computer and computer system	10 years imprisonment or Tk.10 lacs or both.
55	Change of source code of commuter	3 years or Tk.3 lacs or both
56	Hacking with computer system	Extend to 3 years or fine extend to Tk. 1 crore or both
57	Distribution of false, disgusting and defamatory statement or data in electronic structure	Extend to 10 years or fine extend to Tk. 1 crore or both
61	Unapproved access to secured framework	Extend to 10 years or fine extend to Tk. 10 lacs or both

³⁵ ICT Act, 2006; sections 54-66

62	False portrayal and concealing data	Extend to 2 years or fine extend to Tk. 2 lacs or both
63	Disclosure of confidentiality and privacy	Extend to 2 years or fine extend to Tk. 2 lacs or both
64	Distributing false digital mark authentication	Extend to 2 years or fine extend to Tk. 2 lacs or both
65	Publishing false digital mark authentication for fraudulent purpose.	Extend to 2 years or fine extend to Tk. 2 lacs or both
66	Using computer for committing offence	Extend to 2 years or fine extend to Tk. 2 lacs or both

Cyber tribunal:

Section 68 of the Information and Communication Technology Act, 2006 stated that the government of Bangladesh for the quick and compelling transfer of cases under this Act will build up at least one cyber tribunal. The Government will decide the local jurisdiction of the cyber tribunal and will attempt just the offenses under this Act.³⁶The Government will appoint a Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal in consultation with the Supreme Court of Bangladesh.³⁷

The trial system

In two terms the cyber tribunal tries the cyber-crimes. They are:

- 1) With the report of a police officer whose rank isn't below the position of Sub-Inspector.

³⁶ ICT Act, 2006; sections 68(1)

³⁷ Ibid, S. 68 (2)

- 2) With the report of any other person which approved by the controller, or some other individual approved by the controller referenced in the Information and Communication Technology Act 2006.³⁸

The cyber tribunal will follow chapter 23 of Criminal Procedure Code, 1898 (preliminary methodology by the Court of Sessions) so far it is reliable and important to attempt the digital offenders during the preliminary system. If the accused person is being escaped or absconded, then tribunal can attempt the case in absentia. For this situation, the tribunal needs to circular a request in two bangla newspapers to introduce the accused on a predetermined date.

Power of the cyber tribunals

To try the cyber criminals, the Cyber tribunal will apply and follow the arrangements of Criminal Procedure Code and it will have a similar power, a Sessions Court engaged to apply in its original jurisdiction. For this situation, the Public prosecutor will direct the case in the interest of the Government.³⁹

Time limit of the cyber tribunal

The cyber tribunal will finish the trial within 6 months from the date of claim or confining of charge. But if the tribunal thinks fit or necessary, then it may be extends the time for 3 months.⁴⁰

Pronouncement of judgment

The judgment shall be pronounced by the cyber tribunal within 10 days after the ending of prosecution or after the finish of trial which may be deferred for ten days.⁴¹

Cyber Appellate Tribunal

The Government will set up at least one or more cyber appellate tribunal for disposition of the case from the cyber tribunal. This cyber appellate tribunal will be comprised by one chairman and two members who are appointed by the Government. To becoming as chairman of Cyber Appellate Tribunal, the person must be that he was either a judge of the Supreme Court or ought

³⁸ Ibid, S. 69(1)

³⁹ Ibid, S. 70 (2)

⁴⁰ Ibid, S.73

⁴¹ Ibid , S.73

to be a current judge of the Supreme Court or is qualified or fit to be appointed as a judge of the Supreme Court.⁴² One of the two members of the cyber appellate tribunal will be an individual who is retired District Judge or as yet employing in the judicial service of Bangladesh and the other member should be an experienced and skilled person in the case of information and communication technology. They will be selected for 3-5years.⁴³

The Trial System of Cyber Appellate Tribunal

The Cyber Appellate Tribunal won't have any original jurisdiction. The jurisdiction of the cyber appellate tribunal is to just hear and dispose of appeals from the request and judgment of the Cyber Tribunal and suitable cases in the Sessions Court.⁴⁴The decision of the cyber appellate tribunal court will be conclusive and it will hold the ability to modify, hold, alter, retain, revoke, cancel, and annul the request and judgment of the cyber tribunal. If the cyber appellate tribunal isn't built up, the appellate tribunal will pursue or follow the re-appraising methodology of High Court Division of the Supreme Court and the appeal of the cyber appellate tribunal might be heard by the High Court Division.⁴⁵

4.2.3. The Penal Code, 1860

The Cybercrime may involve the criminal activities which are traditional in nature. This activity might be as burglary, extortion, imitation, criticism, defamation, and devilishness, which are part of the penal laws of our nation. The maltreatment of computer has additionally brought forth the extent of new crimes that are led by special laws which sanctioned to punish these types of crime. For instance, Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 characterizes certain offense that doesn't cover by the Penal Code. That is the reason, it might be said that the Penal Code, 1860 isn't powerful enough in managing the cybercrimes in Bangladesh.

4.2.4 The Pornography Control Act, 2012

⁴² Ibid, S. 82 (3)

⁴³ Ibid

⁴⁴ Ibid, S.83

⁴⁵ Ibid, S.84

The National Parliament of Bangladesh has enacted a law in relating to the pornography which is the Pornography Control Act, 2012. The preamble of this Act says that this Act has been figured to prevent the crumbling of good and moral estimations of the general public of our nation.⁴⁶ Information technology gives us some benefits as well as gives some disadvantages if it is utilized by devilishness individuals with criminal goal. Now we can seen extensively in our nation that a video clips, MMS and so on of sex or conduct identifying with sexual exercises which have been recorded on camera by a segment of individuals and afterward it has used to as a blackmail, cheat, defame young girls and women.⁴⁷ Section 2 of the Pornography Act 2012, describe the definition of pornography.⁴⁸Section 5 deals with the investigations procedure and also deals with the other section with the punishment procedure. But there has no any clear provision for dealing with the cyber activity.⁴⁹ This pornography Act has been formulated for those who produce the pornography using a child, man or woman, taking their still pictures, video or film with or without their permission and then print, distribute and publish such materials or sell, supply or exhibit child pornography.⁵⁰

Section 10 of the Pornography Act 2012stated the offence committed under this Act shall cognizable and non-bail able offence.⁵¹ According to section 8(3) of this Act, deals with the punishment which is that if a person is being transmitted any pornography through the internet, website, mobile phone, or any other electronic device, then he will be punished for this offense as long as 5 years and fine up to BDT. 5,00,000.⁵² Therefore, this is not enough to combating the cyber-crime . Because, this Act deals with only deals with the pornography not the issue of cyber-crime

4.2.5 Digital Security Act, 2018

Recently, the Parliament of Bangladesh has been passed the Digital Security Act, 2018 on September 19, 2018.The Digital Security Act, 2018 has been purportedly figured with the

⁴⁶ The Preamble, The Pornography Control Act, 2012

⁴⁷ Md. Sanwar Hossain, The Pornography Control Act, Possibilities and Problems (2012),Law firm in Bangladesh, <http://shossainandassociates.com/oldsite/index.php?p=view-article&article=pornography-control-act>

⁴⁸ Section 2 of Pornography Act, 2012

⁴⁹ Section 5 of Pornography Act, 2012

⁵⁰ Sec. 8, The Pornography Control Act, 2012

⁵¹ Sec. 10, The Pornography Control Act, 2012

⁵² 08 Sec. 8(3), The Pornography Control Act, 2012

aim of guaranteeing the national computerized security in Bangladesh alongside anticipating, controlling and indicting digital offenses, but in practically speaking, it presents huge issue and dangers to free articulation of the people.⁵³ This Act supplanted some of disputable provisions of digital security laws which resemble section 57 of the ICT Act 2006. Section 5 of this Act, deals with the arrangement of Digital Security Agency, who will screen and oversee the computerized issue of substance, correspondences and cell phones to avoid the cyber-crime which committed in Bangladesh.⁵⁴

Section 8 of this Act -deals with the Power to expel or obstruct a few information data which undermines the Digital Security of our nation.⁵⁵ Section 17 of this Act deals with the Punishment for Illegal Entrance in Critical Information Infrastructure which is that in the event that any individual purposefully or intentionally enters in Critical Information Infrastructure,, at that point he will be punished with detainment for a term not exceeding 7(seven) years or fine not exceeding 25 (twenty five) lacs taka or with both. In any case, if any individual deliberately or purposely enters or hurts or destroy or renders inactive the foundation by an illicit methods, at that point he will be punished with detainment for a term not more than 14 (fourteen) years or with fine not more than (one) crore taka or with both.⁵⁶

According to section 18 of the Digital Security Act 2018, if any individual eagerly and unlawfully enters or help to enter in any computer, computer framework or computer network to carry out committed crime and harming something, at that point the individual who perpetrates this crime will be punished with detainment for a term not over 6 month or by fine not more than 3 (three) lacs taka or with both.⁵⁷

According to section 21 which states that If someone by way of any digital medium spread any propaganda or campaign or helps to spreading a propaganda or campaign against the liberation war of Bangladesh, perception of liberation war, Father of the Nation, National Anthem or national Flag of Bangladesh then, the person who commits this crime- he will be punished under the Act, with imprisonment for a term not more than 10 (ten) years or with fine not more

⁵³ New Digital Security Act in Bangladesh deepens threats to free expression,21 September 2018, Access now, <https://www.accessnow.org/new-digital-security-act-in-bangladesh-deepens-threats-to-free-expression/>

⁵⁴ Section 5 of the Digital Security Act, 2018

⁵⁵ Section 8 of the Digital Security Act, 2018

⁵⁶ Section 17(1,2),ibid

⁵⁷ Section 18(1,2),ibid

than 1 (one) crore taka or with both. But If any person commits the offense for the second which mentioned in sub-section (1) then, he will be penalized with imprisonment for the life or with fine not more than 3 (three) crores or with both.⁵⁸ Section 26 states that If any person without any permission or legal authority collects any important information or sells any important information, takes possession, supplies or uses any person's identity information, then-the person will be punished for the first time with imprisonment for a term not more than 5 (five) years or fine not more than 5 (five) lacs taka or with both. Section 27 states that If any person do any crime With the intention to breach the national security of our country or to endanger the sovereignty of the Nation and committing any terrorist activity within the public or a part of them creates obstruction in the authorized access to any computer, computer network or internet network or illegally accesses the said computer, computer network or internet network , then this activity of that person will be treated as the cyber security crime and that's why the person who committed this crime shall be punished with detained for a term not more than 14(fourteen) years or with fine not more than 1(one) crore taka or with both. But, if the activity of that person has been committed for the second time then, he should be punished with detained for a life time or fine not more than 5(five) crore taka or with both.⁵⁹

⁵⁸ Section 21,ibid

⁵⁹ Section 27, ibid

CHAPTER 5

FINDING OF PROBLEMS OF THE STUDY

5.1. INTRODUCTION

In Bangladesh, Cyber and technology related crimes are gradually increasing. At present, Cyber-crime becomes the most serious issue in Bangladesh. Already it has been seen that cyber-crime is a despondent warning which may become visible in the area of information and communication technology. In addition, we also saw that Cyber blustering is becoming a major anxiety for parents because of their children using the internet as their part of the subject by which majority of students in Bangladesh have experienced being disturbed online or being disturbed by the same person both their online or offline. Therefore, cyber-crimes are also becoming a warning to the government itself. In our country, there are only few laws to regulating and controlling the cyber-crime but this is not enough to control this type of crimes. Because of absence of legitimate enactment to control the cyber- crimes, most of the time cyber criminals are safe side after committing such crime. There are several clauses to control the cyber-crime which deals in the Information and Communication Technology Act-2006 and ICT (Amendment) Act-2013. But, this Act isn't concrete and enough against the cyber-crime. So, considering the above facts, there should be introduced and imposed a magnificent and comprehensive Cybercrime Protection Act. On the basis of my research I found some problems that are....

5.1.1. Bangladesh is not safe from cybercrime

Now, Bangladesh isn't safe from cyber-crime in light of the fact that the government measurements for cyber-crime are not extraordinary. The predetermined number of digital crimes caught is kept to email dangers. As indicated by a government study which directed by the Bangladesh Computer Council is that there is just 0.4 percent of the total population of Bangladesh possess having computers and 0.7 percent of the complete population of Bangladesh approach the web. In September 2007, the quantities of internet service providers (ISPs) in Bangladesh were attacked by the Denial of Service (DoS) assault. By this attack causes the

genuine harm. In this situation, our government stays quiet after the assault and they said that we don't have anything to do before media.

5.1.2. Bangladesh is in danger

At present, Cyber terrorists are extremely master than the authority. It is difficult to capture them by the normal police. The framework police power of our nation isn't still developed. Police are not master like American government agency of investigation. For this reasons, it is extremely simple to carry out any cyber-crime in Bangladesh for the cyber criminals. Still we don't have any digital law in our nation. At present, in Bangladesh there is lot of individuals utilizing the Face-book on web. The vast majority of the Students utilizing the face book practically throughout the day. They post unlawful things and publicize it in face-book which made a humiliate circumstance. After that they welcome the students to join such huge numbers of clubs which mainly fake. Along these lines, there is numerous crimes have been committed already by the face-book. Since this site genuinely hampered the education of the students in our nation.

5.1.3. Bangladesh under a serious cyber threat

On August 23, 2004, an email message was sent to Bengali daily Prothom Alo which giving an actual life threat to Awami League president and our honorable Prime Minister sheik Hasina. On August 25, 2004 Another mail was sent to the police central command which additionally containing the existence danger of former Prime Minister Khaleda Zia, her child Tarique Rahman and Bangladesh Nationalist Party (BNP) administrators. For this situation, the police division paid attention to the sends and chose to build up a cyber-crime control unit which unit will be the nation's initially policing unit against cyber-crime. In this issue, two youngsters, a private university student and a software engineer, have been captured in connection with the email undermining the Prime Minister Sheik Hasina and another adolescent for compromising the former Prime Minister Khaleda Zia.⁶⁰In this case the police take assist from the foreign cyber law expert. The Problem is that when the criminal the arrest but there is no law available in our country to deal with this matter. For this reasons it may become very hard for the police to go for the next proceedings. By this result, the police take and find different way to tackle this offence and that is torture which is not supportable. The government still remains silent about the matter

⁶⁰Daily Prothom alo_23 August, 2004

and finding solutions to the threat of cybercrime is a serious and major challenge, mostly for the developing countries.⁶¹

5.1.4 .Use of internet in bad intention

We know that a coin has two sides. Similarly the internet also has two sides which are advantages and disadvantages. So, Internet may be used as a mass destructive weapon. Therefore, a terrorist can destroy one country by using the internet.

5. The Information and Communication Technology Act, 2006 isn't sufficient for dealing with light of cyber-crime.

6 In this Information and Communication Technology Act, 2006 managing just a few sections of cyber-crime yet this isn't clear.

7. The government makes the Digital Security Act 2018 to ensure the cyber-crime yet this is equivalent to the information and communication technology Act 2006. There is no any essential changes will be established.

⁶¹ OECD, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf

CHAPTER 6

RECOMMENDATION

6.1. RECOMMENDATIONS:

First of all, I think it is very important to make a new idea or sense of internet for all and we have to aware about the cyber-crime. As a researcher, I have given some recommendations for obtaining an effective solution on the basis of my research.

- The first task is that we have to realize the problem.
- We have to make a law only for dealing with the cyber-crime.
- The government of Bangladesh should to make a cyber-forensic.
- The law enforcer bodies should be more expertise than the cyber criminals.
- High punishments ought to be upheld for the individual who carried out the cyber-crime and the individual who don't report the occurrence of cybercrime.
- Should be maintained the proper training and awareness to citizens, organizations, the Government and public in general dealing with the gathering of digital forensics evidences; and how to report cybercrime.
- The Government of Bangladesh should change the National ICT arrangement to make up new ICT advancements in the business.
- Should be used the strong password. The password should be the combinations for different accounts and should be avoid writing in simple word.
- The password or accounts should be changes on a regular basis.
- Use of active firewalls, IDS, IPS, refreshed antivirus and anti-spyware and blocking the spyware attacks.
- We have to make sure that our social networking profiles are set to private and savvy. (Face-book, You Tube, Twitter etc.)
- We have to secure of our mobile devices.
- Should be secure of our wireless network.
- Should be protected of our e-identity.
- We want a cyber –store-house.

- We have to establish an internet based education.
- Raising the public awareness which is very important to implement in this law.

If we establish above this recommendations, then I think we can make a safe house of internet at last.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

The present conceptual system has been given a concise outline of approaching attempts to avert and control the innovation and computer related crime which featuring the general fitness or pattern and improvement inside or outside the financial area of Bangladesh. Despite the fact that, Internet and web advances are becoming so quick in the present world yet they are giving new chances and they are additionally comprising of specific dangers like-email undercover work, MasterCard misrepresentation, spam's, programming robbery, and so on. Therefore should be careful about it. Cybercrime is obviously the new dimension form of the crimes at present in the world which is very tough to suppress. But, it will not be difficult to prevent us to take adequate measures for controlling against the cyber-criminals. It is high time to control and prevent the upcoming cyber threats of Bangladesh and other related issues. By the proper and effective measures of the government and rising the awareness among the people- cyber-crime s can be reduced and control. The common people or citizens should be cautious in utilizing computer frameworks and online offices. The nation ought to take every single imaginable measure to anticipate any kinds of digital attack which may place the lives of individuals in a tough situation. There is likewise an important to get any progressions in the Information Technology (ICT) Act and Digital Security Act to make it progressively viable to battle cyber-crime. The general individuals ought to likewise be cautious while utilizing the PC frameworks and online offices. So we trust that our mindfulness and steady challenge digital wrongdoing will bring about progress.

SELECTED BIBLIOGRAPHY

Statutes

1. The Information and Communication Technology Act, 2006
2. The Penal Code, 1860
3. The Code of Criminal Procedure, 1898
4. The Pornography Control Act, 2012
5. The Digital Security Act, 2018

Books

1. Karzon, Sheikh Hafizur Rahman, Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, 2008, page 249-252. Page-411-418
2. Yar, M. The novelty of cybercrime: An Assessment in Light of Routine Activity Theory, European Society of Criminology, 2005, pages 407-427
3. Edwin H. Sutherland, Principles of Criminology, Second Edition, Philadelphia: Lippincott, 1934, page 3
4. Monjur Kader, theory and practice of criminology Bangladesh perspective, 2015, 245-265

Online Journals

1. Goodman/Brenner, the Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70
2. Goodman, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol.10, No.3
3. ABA International Guide to Combating Cybercrime, 2002, page 78
4. Computer Law Review International, 2006, page 142
5. Gerick, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International 2008, page.

Online Books

1. Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber-crime and Terror, Seymour/Goodman, page 225
2. Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA3, page 3
3. Gercke, the Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, 141
4. B.Magalla, the New Era of Cyberspace: Their Protection, Prevention and Detection. Tumaini University Iringa University College, 2013

Website links

1. <http://saber.eaber.org/sites/default/files/documents/Bangladesh%20Vision%202021.pdf>
2. <http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>
3. <http://gadgets.ndtv.com/internet/news/bangladeshis-hack-20000-indian-websites-224516>
4. <https://edition.cnn.com/2012/09/30/world/asia/bangladesh-muslim-buddhist-violence/>
5. www.oecd.org/dataoecd/5/47/34935342.pdf
6. <https://www.accessnow.org/new-digital-security-act-in-bangladesh-deepens-threats-to-free-expression/>
7. <https://www.thedailystar.net/law-our-rights/cyber-crimes-70592>
8. <https://www.techopedia.com/definition/24841/denial-of-service-attack-dos>