



UGC & Govt. Approved
Sonargaon University (SU)
সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph

On

"Prevention of Cyber Crime in Bangladesh"

This Research paper is submitted in partial fulfilment of the requirement for the degree of **Master of Laws (LL.M.)** under Sonargaon University.

SUPERVISED BY:

Sharmin Jahan Runa

Assistant Professor & Head of the Department

Department of Law

Sonargaon University

SUBMITTED BY:

EASHIN MOLLAH

Student Id: LLM2502033002

Department of Law

Sonargaon University



Date of Publication: 25 June 2026

DECLARATION

The researcher, as a candidate for the degree of **Master of Laws (LL.M.)** is fully aware of the rules and regulations of the Sonargaon University relating to the preparation, submission, retention and use of a research monograph. He acknowledges that the University requires the research monograph to be retained in the library for record purposes and that within Copyright privileges of the author it should be accessible for consultation and copying at the discretion of the library authority and in accordance with the Copyright Act 2000. I authorise the Sonargaon University to publish an abstract of this research. The researcher also declares that this research monograph entitled.

Prevention of Cybercrime in Bangladesh: A Critical Analysis of Prevention of Cybercrime in Bangladesh, is solely the outcome of her own efforts and research for the partial fulfillment of the degree of **Master of Laws (LL.M.)**. No part of this research monograph in any form has been submitted to any other department or institution for the award of any degree or diploma or to any journal for the purposes of publication.

Eashin Mollah

Student Id: LLM2502033002

Batch: LL.M. 33rd

Department of Law

Sonargaon University.

ACKNOWLEDGEMENT

All praises are for **Almighty Allah** who has given me the opportunity and ability to conduct this research. His special grace and blessing, in fact enabled me to complete this work within such a sort time. I would like to express my deepest appreciation to my **respected Teacher** for his proper guidance, valuable suggestions, and very useful comments on the earlier drafts and constant encouragement during the whole period to complete research monograph. Without his help it would not be possible for me to carry out this paper.

Finally, I offer my cordial thanks to my Teacher of research and well wishers especially for their assistance in various ways in compilation of this research monograph

Eashin Mollah

ABSTRACT

This research is based on cybercrime only. The governments across the world, police departments and intelligence units have started to react to cybercrimes. This study provides an overview of cybercrime and examines awareness in different respondents on the issue of cybercrimes in Bangladesh as well as emphasizes the severity of the problem and the urgent need to limit its impact worldwide. It is pertinent to mention that without creating a precise legal framework enabling law-enforcement agencies to identify cyber offenders and prosecute them it is almost impossible to prevent cyber-attacks and cybercrimes in Bangladesh. Here also described the internet uses and its bad impact. The process of combating cybercrime is described here and the implementations of laws are shown in it. This thesis is totally based on laws of our country. It also focuses the lacings of our laws and how to solve this problem; it also described. How to combat cybercrime and by which way; it also mentioned here. Describe the combating system, which is mentioned in our Acts. What is the scenario of our country; also shown in this. Bangladesh is not capable to combat it now; it is proved in this research and the way of overcome from this is also mentioned. We have no any laws to combating cybercrime and why it is urgent to make it; also elaborate in this research.

The present technical protection measures in the prevention of cyber-crimes in the country there are many circles and cases wherein such technology is not available or failed or circumvented by a number of barriers. To remove all such obstacles, the existence of a proper legal frame-work is of great importance for recreating and maintaining cyber-security.

TABLE OF CONTENTS

DECLARATION

ACKNOWLEDGEMENT

ABSTRACT

LIST OF ABBREVIATIONS

Chapter-01

General Introduction

1.1 Introduction.....	7
1.2 Historical Back ground of Cybercrime in Bangladesh.....	7
1.3 What exactly is cyber.....	8
1.4 Statement of problem.....	9
1.5 Chapterization.....	10
1.6 Conclusion.....	10

Chapter-02

Aims and Methods of the Study

2.1 Introduction	11
2.2 Aims and Objectives of the Research	11
2.3 Literature review.....	12
2.4 Justification or rational.....	13
2.5 Scope & Limitations.....	13
2.6 Research Methodology.....	13

2.7 Conclusion.....	14
---------------------	----

Chapter-3

Different types of Cybercrime in Bangladesh

3.1 Types of Cybercrime	15
3.2 Cyber Crimes against Property	16
3.3 Cybercrimes against Government	17
3.4 Cybercrimes Against Society at large	17
3.5 Present Situation.....	17

Chapter 4

Cyber Laws in Bangladesh

4.1 Introduction	20
4.2.1 Information and Communication Technology Act, 2006.....	20
4.2.2 This Act declared following activities are Cybercrimes	21
4.2.3 Limitations of the said Act.....	21
4.3 Digital Nirapotta Ain 2018.....	22
4.3 Cyber Tribunal	23
4.4 Cyber Appellate Tribunal	24
4.5 Pornography Act 2012 and Child Pornography	24
4.6 Penal Code 1860.....	25
4.7 Bangladesh Telecommunication Act 2001.....	26
4.8 Cyber Crime Report.....	26

Chapter 5

Challenges for Implementation or Combating Cyber Crime

5.1 National Plan	28
5.2 Law Makers on the Basis of Cyber	29
5.3 Law Ministry on the Basis of Cyber	29
5.4 Public Awareness about Cybercrime	29
5.5 Internet Based Education	29
5.6 Digital Security	30
5.7 Investigational Power and Investigational System.....	30

Chapter 6

Findings, Analysis, Recommendation & Conclusion

6.1 Introduction.....	31
6.2 Findings.....	31
6.3 Critical Analysis.....	32
6.4 Recommendations.....	37
6.5 Conclusion.....	37

Bibliography

Chapter-01

General Introduction

1.1 Introduction:

Cybercrime is still a low priority in Bangladesh. Though computers are becoming common house hold items and the numbers of internet users have already crossed thirty millions, very few computer related offences are reported to the police. In Bangladesh there is no Computer Emergency Response Team (CERT), no cyber police or virtual police to handle the incidents such as computer abuses, hack attempts and other information security breaches. Bangladesh has enacted the Information and Communication Technology ACT of 2006 (Act no 39 of 2006) with a maximum punishment of 14 years of imprisonment or maximum fine of 10 million taka (Bangladeshi currency) or with both for a cyber-crime. Still the legislation seems not to be sufficient to effectively fight cyber-crimes in the country. The present Government is expected to invest millions of taka to materialize its promise to build a digital Bangladesh. This is why the issue of prevention of cyber-crime must get due priority and a considerable portion of budget should be allocated to ensure the issue. This chapter finds the policy of prevention of cyber-crimes in Bangladesh and also provides some sort of recommendations.

1.2 Historical Back ground of Cybercrime in Bangladesh:

Bangladesh, despite being a third world country, has seen a technological revolution. A Bangladeshi teenager has very easy access to computers and other devices. And so, they get enough opportunity to engage in hacking. Hacking has already become a major problem in Bangladesh. Young people are getting more and more interested in hacking for the thrill in it. Not just young people, even the mainstream media is so often engaged in the hacking and exposing private information.

The Mahmudur Rahman case is one of the leading cases in terms of cybercrimes in Bangladesh and may be referred as the first cybercrime case in Bangladesh. Mahmudur Rahman, the founder of a Bangladeshi newspaper named Amar Desh was sued in line with a High Court directive for publishing reports on Skype conversation between former International Crimes Tribunal chairman Justice Md Nijamul Huq and an expatriate legal expert in December, 2012. He was sued along with the Amar Desh publisher Hashmat Ali on December 13, 2012.

On 15/02/2012 a group of alleged Bangladeshi hackers named 'Black HatHackers' hacked more than 25000 Indian webs ites which included important sites suchas the website of the Border Security Forces (BSF). Propaganda activities are alsoconsidered as cyber-crimes in some instances. Propaganda is information which is biased and misleading in nature used to promote or publicize a particular political causeor ideology. It creates agitation and panic among the public.

For example, we can mention the 2012 Ramu Violence in Cox's Bazar. Someone with a fake Facebook account posted a photo of desecration of the Holy Quran on its wall. The fake account was under a Buddhist male name. This post agitated the common Muslim people of that area and they, without verifying the authenticity of the Facebook account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were destroyed. 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 worsen.

1.3 Cybercrime exactly what is :-

- "A wide range of malicious activities, including the illegal interception of data,system interferences that compromise network integrity and availability, and copyright infringements."¹
- In 1997, John Carlin wrote an article for the Wired Magazine titled'A Farewellto Arms' . While Ernest Hemingway's novel of the same name tells about a soldier literally bidding farewell to arms, John Carlin's article presents a completely different scene. In his article John Carlin brought forth a new idea.What he meant to say is that future wars won't require conventional weapons.Instead they will be fought in another way. The way he foresaw nearly twodecades ago is the reality of today.
- "Offences that are committed against an individual or group of individuals witha criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly usingmodern telecommunication networks such as internet (chat rooms, emails,notice boards or groups) and mobile phone (SMS/MMS)."²

¹ The Council of Europe Convention on Cybercrime

² Dr. Debarati Haldar and Dr. K. Jaishankar

- “Cybercrime is taking a bottom-line toll on the corporate workplace. Last year, losses exceeded \$100 million and that figure continues to skyrocket as security breaches pose an increasing threat to U.S. corporations, banks, and even the government”.³

Cyber criminals are most commonly known as hackers. The term “hacker” is now so overused that it has come to be applied to anyone who breaks into computer systems. But this is not entirely correct. There is a difference between hackers and crackers, although the term “cracker” has never caught on with general public.

Hackers are people who gain unauthorized access to computers or telecommunication systems, often just for the challenge of it. They think it as a challenge which they accept for fun. Some of the hackers even believe and vigorously claim that they are performing a service by exposing weaknesses and security flaws of various computer networks. These hackers are not interested in obtaining anything or have no motivation for financial gain, shut down hardware pirate software or alter or destroy data. They often engage in sabotaging the victim’s assets. The aforementioned hackers are colloquially called ‘white-hat hackers’ (who are not malicious) and those mentioned later are called ‘black-hat hackers’ (who are malicious).

1.4 Statement of problem:

To build a secure field of cyber home, it is very important to make a body. Who have much knowledge of internet and other such issues, which are relate with the technology. This research is very important to encourage the government to build up that safety house. If we make a body only for the protection of this sector and if we maintain a strategy like-“every person who wants to access internet, he/she have to maintain a rule, then we can make a net for trap the offender easily. The rule is- each and every person should register for access internet by their national identification number or by their birth certificate number”, then they can access. Otherwise they won’t. By this way no one can make any twice ID number in any site (as like social media sector, official sector, government sector etc.). And all access are recorded and reserved. Some other rules are also important that, when any one access any red marked page then a notification will reach in the security house, and then the agency can easily arrest the offender and after that we can apply the other Acts easily to prevent the cybercrime. For that reason, I think it is very important to research on this field.

³ Beth Wilson

1.5 Chapterization:

The thesis has been divided into six chapters, as follows:

The first chapter is an introductory part of the study. The second Chapter deals about Aims and Methods of the Study. The third chapter deals about the Different types of Cybercrime in Bangladesh. The fourth chapter deals with the Cyber Laws in Bangladesh, The fifth chapter deals with the Challenges for Implementation or Combating Cyber Crime and the sixth chapter is General Findings, Analysis, Recommendation & Conclusion.

1.6 Conclusion:

In a few words it stated that, this research is specifically based on prevention of cybercrime in Bangladesh. This is the very important analysis for our country. Till 1996 to till today the crime in the cyber sector is very high and day by day it across beyond our statute law. We should stop it, for that reason it is an initiative analysis for solve it.

Chapter-02

Aims and Methods of the Study

2.1 Introduction:

Everything has an aim and objective, and has a specific methods on which it will be done. This is the important part of a research, which deals about literature review, statement of problem, aims & objectives, Justification or rational, scope, limitations and methodology.

2.2 Aims and Objectives of the Research :

It is always emphasized that a problem usually comes with its own seeds of solution. This statement signifies the need of defining the objectives of the research. The main objective of the research is to come up with an important solution that may curb cybercrimes in Bangladesh. In order to achieve this goal, the awareness of the problem of cyber-criminal activities among the people of the country is a must. People must understand how the internet as well as the cyber world operates. The growing danger arising from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. This study investigates whether or not people would use the Internet to report cybercrimes. Main objective, therefore, of the study is to develop an awareness of cybercrimes among the people as well as to design the way outs and the measures to control and prevent cyber-crimes and address the recommendations to mitigate the loopholes of cyber-laws of Bangladesh. In this study, some arguments are also intended to be set out in the research-work that can provide links to academic and other material so as to shed light on the examination of the issue of prevention of cyber-crimes in Bangladesh perspective.

- To find out the importance of cyber-Crime in Bangladesh and all over the world;
- To find out the existing problems of cyber law in our country to control cyber-crimes.
- To know about cyber-crime in Bangladesh details.
- To promote effectiveness of the government and law enforcing agencies to control cyber-crimes.
- To identify the ways of making control over cyber-crime to stop the great loss of economy.

- To find out the root causes for the rising cybercrime in Bangladesh.
- To know about the existence the cyber security in Bangladesh.
- To know the causes of the involvement of crime in the cyber security term.
- To know what is the effect to family and society for increasing cybercrime?
- To know way the reducing cybercrime in Bangladesh.
- To know how men involve with cybercrime?
- To find out the way to protect important information or data from the hacker in the cyber security.

2.3 Literature review:

This is a research which based on, "Prevention of Cyber Crime in Bangladesh". Many men define the Cybercrime and control, based on their experience. Many people define, "what is cybercrime?" But I think some materials are missing in their research, that is, "Have any specific body to control it? I think their definition is not clear on the basis of this question". Now a day's many cases are filled on the basis of cybercrime. Sufi Faruq Ibne Abubakar, only one person; who write on this topic only in his article.

He said that, "The concept of a Digital Bangladesh is welcomed by the IT professionals and the general mass. To fuel this notion the government must give due importance to the matter of cybercrime. Otherwise, like many other positive initiatives this will fall on its face. It is a matter of hope that the "National Information and Information Technology Guidelines 2009" has included Cybercrime as an agenda. To make this a success the Ministry of Information Technology, along with the IT professionals and the media must come forward"⁴

In Bangladesh perspective we have a law, based on cybercrime is ICT Act 2006 & Digital Nirapotta Ain-2008. But these are not sufficient to reduce cybercrime. We have to a body which can control it. There are many loopholes in our Acts. The use of internet has become the part and parcel of every educated person in this world. But it is to disagree with him that, now a day's not only educated person but also an illiterate person involved with the internet. For that reason, they won't detect which is the harmful web, and doing unlawful activities. But they aren't well known about the proper use of internet. In the other side some bad people which are educated and also some are illiterate voluntarily held such illegal activities in the internet. Now a day's any person can inter in the internet very easily, but if we have a body for control

⁴ <<http://sufi-faruq.com/en/combating-cybercrime-a-bangladeshi-perspective-2/>>

the field of internet and make some hard rules for access internet, then we can reduce the illegal activities in that field.

2.4 Justification or rational:

By this research society can receive a peaceful cyber world, I think. But this is not sufficient for make a better cyber world. Have some more initiative step to make it. By make it, we can ensure employment of some persons, who are unemployed. Not only this but also we can protect the person who are accessing in internet. People can easily find right things not a vogue. I think child also safe from bad things, they have no any chances to manipulate. Social media also protected by this. All official sectors also besecured from hacking. It is very initiative step to make it.

2.5 Scope & Limitations:

The scope of the study relates to the present conditions regarding cyber-crimes in Bangladesh. As the scope of cyber-crimes are wider than any other offences, so the researcher go through about the well-known offences which are commonly occurred inBangladesh and preventive measures of those crimes . The scope of the study also will be limited within present laws of Bangladesh with in the essence of International laws Due to constraint of time and non-availability of necessary documents relating to cyber-crimes in respect of Bangladeshi cyber offences ,the study is limited in respect of time and place as mentioned above. Beside all of these, there are lots of limitation for conducting a research work in Bangladesh. Some are given below:

1. Lack of Secondary data.
2. Respondents were not very much interested.
3. Scarcity of time.
4. Survey are limited.
5. Funding are not sufficient.
6. Student's unwillingness to explore their own view.
7. Difficulties to getting appointment of participant.

2.6 Research Methodology:

The whole research paper has been done in an organized way. First, necessary divisions have been selected. Cyber Crime Investigation and Trial Procedure in Bangladesh. The Methodology followed though the research paper has been point out below:

- To make a plan for the whole research paper.
- To divide the whole research paper into different parts.
- To take active from honorable Teacher.
- To study the document.
- To collect material for internet.

2.7 Conclusion:

In a few words it stated that, this research is specifically based on prevention of cybercrime in Bangladesh. This is the very important analysis for our country. Till 1996 to till today the crime in the cyber sector is very high and day by day it across beyond our statute law. We should stop it, for that reason it is an initiative analysis for solve it.

Chapter-3

Different types of Cybercrime in Bangladesh

3.1 Types of Cybercrime:

There are many kinds of cybercrimes. Some of them are briefly mentioned below-

- **Hacking:** It is an offence to hack a computer system which belongs to other individuals or organizations. Hacking puts the victim in a very vulnerable position as there are risks of exposing all the confidential information in a computer system. It is a punishable offence and the laws regarding hacking are quite strict.
- **Cyber-defamation:** The internet can be used to spread misinformation just as easily as information. Websites can present false or defamatory information especially in forums and chat rooms, where users can post messages without verification by moderators. It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a world wide range.
- **Cyber-extortion :** Cyber-extortionists create harmful soft-wares and often threaten individuals or organizations. With those soft-wares they can cause serious damage to the threatened individuals or organizations. They offer 'protection' in exchange of money otherwise they destroy or expose all financial and security information. These cyber-extortionists can be regarded as the new age cyber-mafias.
- **E-mail bombing:** E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account (in case of an individual) crashing. This kind of things are done to harass someone purposefully.
- **Cyber-terrorism:** The term cyber-terrorism was coined in the 1980s by Barry C. Collin. It is defined as the premeditated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Cyber-terrorists can do unimaginable harm to a group of people or a state. They can get into a telephone network during an emergency and shut it down causing more casualties. Suppose, a situation similar to 9/11 has arisen and emergency personnel are being deployed. Meanwhile, the terrorists can hack into

emergency communication system and redirect all orders, give false information etc. Thus, the situation will worsen. In USA, FBI has a separate Cyber Security Unit (CSU) who works to protect the nation from such attacks. Cyber-terrorists target transportation, telecommunication, financial data etc. Thus, a war can be won without shooting even a single bullet.

- **Virus Dissemination Virus:** Virus Dissemination Virus itself is software that attacks other software. It may cause for data loss, deduction of bandwidth speed, hardware damage etc. Trojan Horse, Time Bomb, Logic Bomb, Rabbit are the malicious software.
- **Software Piracy :** Theft of software through the illegal copying of genuine programs or distribution of products intended to pass for the original.
- **Pornography:** Pornography is the first consistently successful e-commerce product. Deceptive marketing tactics and mouse trapping technologies pornography encourage customers to access their website. Anybody including children can log on to the internet and access website with pornographic contents with a click of a mouse.
- **Credit Card Fraud:** You simply have to type credit card number into www page of the vendor for online transaction. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner. Through falsification of computerized bank accounts cores of taka may be misappropriated. In some cases people are arrested and charged for stealing and misusing credit card numbers belonging to others.
- **Sale of Illegal Articles :** Narcotics, weapons and wild life etc. are sold by posting information on websites, auction websites, and bulletin board or simply by using email communication. Many of auction sites are believed to be selling cocaine in the name of money.
- **Online Gambling:** Millions of websites are offering online gambling which are believed to be actual fronts of money laundering. Though it is not yet confirmed, these sites may have relationship with drug trafficking.
- **Intellectual Property Crimes :** These include software piracy, copyrights, infringement, trademark violations, theft of computer source code etc.
- **Cyber Defamation:** With help of computers and/ or the Internet When any defamation takes place it is called cyber defamation. It can tarnish personal image of any individual or reputation of any company, bank or institution.

3.2 Cyber Crimes against Property:

As there is Rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affect person's property are as follows:

1. Intellectual Property Crimes
2. Cyber Squatting
3. Cyber Vandalism
4. Hacking Computer System
5. Transmitting Virus
6. Cyber Trespass
7. Internet Time Thefts

3.3 Cybercrimes against Government:

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

1. Cyber Terrorism
2. Cyber Warfare
3. Distribution of pirated software
4. Possession of Unauthorized Information

3.4 Cybercrimes Against Society at large:

An unlawful act done with the insertion of causing harm to the cyberspace will affect large number of persons. These offences include:

1. Child Pornography
2. Cyber Trafficking
3. Online Gambling
4. Financial Crimes
5. Forgery

3.5 Present Situation:

Charges proven in 15 out of 495 cases, Criminals continue to victimize people online, with conviction rates reported to be as low as 3% in cybercrime cases, under the now defunct Information and Communication Technology (ICT) Act. "It was found that charges against the accused were proven in only 15 out of 495 cases, where the accused in 480 cases were relieved

of charges since the tribunal's inception in February 2013".⁵ Of the cases, police submitted the final report in only 129 cases before the tribunal. The accused were released as charges were not proven. The accused were discharged at the outset in 83 cases during charge framing hearings, when the court found the probe reports to be faulty. In another 54 cases, the accused were acquitted when the prosecution failed to prove charges against them. Most of the accused are released mostly due to out of court settlements, lack of skilled lawyers, and the inexperience of law enforcement in handling cybercrime cases.

"Cybercrimes are reported every day in the country. 2,044 cases were filed with different police stations and the cyber tribunal in the last six years. The court received 925 cybercrime cases in 2018, and as many as 130 cases in the first two months of 2019".⁶ The number of cybercrime cases was only three in 2013, but it went up to 33 in 2014, 152 in 2015, 233 in 2016, and 568 in 2017.

For instance, On January 5, 2017, a case was filed with Mohammadpur police station against cricketer Arafat Sunny by Nasrin Sultana, on charges of threatening to reveal indecent photos of her on social media sites. Nasrin claimed to be Arafat's wife. During the trial, Nasrin and Sunny settled the matter out of court and later on April 24, 2018, the tribunal acquitted the accused, saying the prosecution had failed to prove the charges. On February 22, 2015, two youths, Md Rasel Mia, 21, and Din Islam, 25, assaulted a schoolgirl on her way to a coaching centre in Bhaluka upazila of Mymensingh. Later, the accused posted compromising photos of her on social media.

The investigation officers and prosecution cannot establish charges against accused cyber criminals due to lack of skill and efficiency required in handling these cases. They said cybercriminals are increasing alarmingly across the country as loopholes in the law let these criminals off the hook. It was found that the judge in many verdicts said the accused were acquitted since the prosecution could not prove charges beyond doubt in these cases.

In many cases, the investigation officer often submits a charge sheet without relevant and important evidence. The court then discharges an accused, not having any substantial or relevant evidence against him/her. "The investigation officers submit weak investigation reports due to poor knowledge. This is why it becomes difficult for the prosecution to prove charges."⁷ Most cases filed under the ICT Act are being filed just for harassment and the conviction rate is poor. The conviction rate was very poor due to out of court settlements, and

⁵ Cyber Tribunal (Bangladesh) in Dhaka

⁶ Cyber Tribunal (Bangladesh) data.

⁷ Barrister Jyotirmoy Barua, with experience in a good number of cybercrime cases.

faulty police probe reports due to lack of skills in handling digital crimes. The police often submits charge sheets in cybercrime cases without IT and forensic reports.

There aren't enough laws in Asian nation which can penalize the cyber criminals. In Bangladesh court there's a law named "The Bangladesh Information & Communication Law 2006" (As amended in 2009). During this law section 56(1) has declared the penalty of ten years imprisonment with or without fine.

Section sixty eight of the aforesaid act has declared the formation of a special court named "Cyber Tribunal". World Health Organization might take cognizance of such forms of Cyber Crime however it's nevertheless to stop or penalize the criminals. It's not nevertheless reward any quite penalty.

Due to the insufficiency of trained specialist aiding the court it's become substantially not possible for the court to trace the crime furthermore because the criminal and to penalize him. There's solely a cyber-judicature in Dacca town established underneath section eighty two of the aforementioned act. This judicature has not nonetheless reward any social control to any criminal. Out of this until to the institution of Cyber judicature within the district court the Session court has the cognizance to trial such reasonably crime underneath section seventy four of the aforementioned act.

In Asian nation there's a statutory authority named BTRC that perform as a watchdog in cyber protection however it's nonetheless to satisfy its guarantees. It's the authority to conduct mobile courts with the assistance of alternative government organs for the speedy trial of such reasonably crime.

Development of Science and ICT depends on the growth of telecommunication sector. This sector remains below developed attributable to lack of liberalization and open competition. The impact of cybercrime isn't fearful Bangladesh as a result of money transactions haven't nevertheless been totally expedited in on-line.⁸

As presently as money transactions are allowed online pc crimes can increase at new rate unless the govt. acquires the tools and infrastructure to forestall, notice and prosecute them.⁹

But our government still not awake to the very fact. Web services provided through the native space network are liable to similar attacks and intrusions by hackers a lot of usually once the protection level is insufficient. Currently every day in Bangladesh some individuals send

⁸ Freddy Tan, chief security advisor of Microsoft Southeast Asia give this statement in a seminar on 10 September 2006 at Dhaka.

⁹ The Financial Express (10 January 2008).

malicious mail to completely different foreign commission and alternative VIPs that generally cause major problem for the police and additionally for the govt.

Chapter-4

Cyber Laws in Bangladesh

4.1 Introduction:

Crime In order to facilitate e-commerce and encourage the growth of information technology, the ICT Act, 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or with both. However, recently our Parliament amended the ICT Act 2006, raising penalties for cybercrimes setting a minimum of 7 years imprisonment and a maximum of 14 years or a fine of Tk. 1 core or both. The Information and Communication Technology (ICT) Act, 2006 came in force on 8 October, 2006. Subsequently, the government amended the Act in 2008 and in 2009. For the better application of the Act, the government passed Information Technology (Certificate Authority) rules in 2010. But these laws alone are not enough. To face the challenges growing in cyber space it is essential to amend the existing laws such as the Penal Code 1860, the Evidence Act 1872, the Contract Act 1872 etc. It is hoped that these Acts will be modified in accordance with the demand of time.

4.2.1 Information and Communication Technology Act, 2006:

There are some provisions in the ICT Act, 2006 which mention penalties for various cyberspace related crimes. For instance, section 54 (1) of this Act declares the offences concerning cyber space. Then, section-54(2) says, "If any person commits offences under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka ten lakhs, or with both". We can also look at section-56 which says-

"If any person—

- (a) with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any

information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

- (b) damage through illegal access to any such computer, computer network or any electronic system which do not belong to him; then such activity shall be treated as hacking offence ;
- (c) whoever commits hacking offence under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka one crore , or with both.”

We can see that law has taken the matter of cyber-crimes in consideration and there are some strict rules regarding it.

4.2.2 This Act declared following activities are Cybercrimes:

- Unauthorized copying, extracting and downloading of any data, database
- Introduction of virus
- Damage and disruption to computer system and computer network
- Denial of access to authorized person to computer
- Providing assistance to make possible to commit to crime
- Hacking with computer system
- Tampering computer source documents
- Electronic forger for the purpose of cheating and harming reputation
- Using a forged Electronic record
- Publication of digital signature certificate for the fraudulent purpose
- Confiscation of computer, network etc.
- Publication of information which is obscene in electronic form
- Misrepresentation and suppressing material facts for obtaining digital signature certificate
- Breach of confidentiality and privacy
- Publishing false digital signature certificate

4.2.3 Limitations of the said Act:

Critics point out that still there remain certain specific limitations of the said Act as under:

- 1) The Act remains silent about various intellectual property rights like copy right, trade mark and patent right of e-information and data.
- 2) The enactment has a major effect on e-commerce and m-commerce in Bangladesh. But it is self-mum as to electronic payment of any transaction.
- 3) The legislation was initially supposed to be applied to crimes committed all over the world; but nobody knows how this can be achieved in practice.
- 4) Spamming has become a peril in the west as such they have made anti-spamming provisions in cyber law. However, there is no anti-spamming provision in our Act.
- 5) Domain name is the major issue which relates to the internet world thoroughly. But the ICT Act, 2006 does not define 'domain name' and the rights and liabilities relating to this.
- 6) The Act does not address any crime committed through using mobile phones.
- 7) This law made e-mails as evidence, conflicting with the country's Evidence Act that does not recognize e-mails as evidence.

We hope our government would take proper initiative to get rid of the problems by ensuring a cybercrime free peaceful society.

4.3 Digital Nirapotta Ain 2018:

This Act is an upgraded version of the cyber-protection law of the country, and will replace some of the controversial provisions of cyber-security laws, like section 57 of the ICT Act 2006. Some basic features of the Digital Nirapotta Ain 2018-It recognizes and defines E-Commerce, E-Transactions. In section 4 of the Act illustrates the jurisdiction of the Act, which covers both persons within and beyond the borders of Bangladesh.¹⁰ Section 5 says about constitution of a Digital Security Agency, who shall monitor and supervise the digital contents, communications mediums including mobile phones to prevent cyber-crime. This section also introduces Digital Forensic Lab and Bangladesh Cyber Emergency Incident Response Team (Bangladesh-CERT).¹¹ Section 13 of the Act illustrates the Power of the DG of Digital Security Agency, where the DG can order a ban on communication in extra-ordinary situation (security breach or national-international threat) to any individual or service provider.¹² In that case, the person or service provider has to facilitate the interception, monitoring and decryption of the Computer or source. It says the Act illustrates the cybercrimes in form of Hacking, impersonation, violation of privacy and other ways, on the basis of section 15.¹³ Section 15(5) of the Act says, any derogatory comments, remarks, campaign or

¹⁰ Section 4 of Digital Nirapotta Ain 2018

¹¹ Section 5 of Digital Nirapotta Ain 2018

¹² Section 13 of Digital Nirapotta Ain 2018

¹³ Section 15 of Digital Nirapotta Ain 2018

propaganda in electronic media made by a person, institution or foreign citizen, against the war of liberation, or father of the Nation Bangabandhu Sheikh Mujibur Rahman or any issue that has been settled by the Court shall amount to an offense under this Act.¹⁴ Section 36 of the Act describes the offense under this section as cognizable and non-bailable.¹⁵ In section 16 illustrates the Punishment for the offenses under section 15 (cybercrimes, propaganda against Liberation War or Bangabandhu), ranging from 3 years Prison sentence to Life Imprisonment and/or a fine of 10 Million taka.¹⁶ In section 21 encompasses the similar offense of any person who aids or abets the commission of any offense under the Act, and shall be entitled to similar punishment.¹⁷ The trial under Digital Nirapotta Ain 2018 shall be held on the same Cyber Tribunal that was established under the ICT Act 2006; the procedures of the Tribunal shall be similar as well concluding the trial within 180 days.

In clearly I explain that the section 2 of Digital Nirapotta Ain 2018 defines that what is lawful access, unlawful access, critical information infrastructure, e-transaction, e-payment, data corruption, data, program, digital network, subscriber information, traffic data, electronic forgery, digital pornography, digital child pornography etc.¹⁸ But in other section describe to storage and archiving the documents. But how storage it is not mentioned in this Act. Here is 30 percent laws are new but least 70 percent are repetition of other laws like ICT Act, Penal Code and Code of Criminal Procedure. Where to recruit the officer to maintain the sector is not clearly define in this Act. Here also some lacking that the Police also act as also this sector and investigate it but I think here the IT sector specialist should recruit as a law enforcement agency to control this sector.

The 1st judgment under this Act has given recently on 29 November, 2019 by Judge Ash Sams Joglul Hossain of the Cyber Tribunal of Dhaka, in **Nusrat Jahan Rafi vs State Case. Moazzem Hossain**, former officer-in-charge of Sonagazi Police Station, was sentenced to eight years of rigorous imprisonment. In this case filed for filming madrasa student **Nusrat Jahan Rafi's** statement and circulating the video clip on social media without her consent. He was also fined Tk 10 lakh, in default of which he has to serve six more months in jail.¹⁹

4.3 Cyber Tribunal:

¹⁴ Section 15(5) of Digital Nirapotta Ain 2018

¹⁵ Section 36 of Digital Nirapotta Ain 2018

¹⁶ Section 16 of Digital Nirapotta Ain 2018

¹⁷ Section 21 of Digital Nirapotta Ain 2018

¹⁸ Section 2 of Digital Nirapotta Ain 2018

¹⁹ The Daily Star, Saturday, November 30, 2019

According to section 68 of the Information and Communication Technology Act, 2006 for the speedy and effective disposal of cases under this Act, Government shall establish one or more cyber tribunal. The tribunal shall try only the offences under this Act and the Government shall determine the local jurisdiction of the tribunal. In consultation with the Supreme Court, Government shall appoint a Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal. Cyber tribunal shall take a case for trial— upon the report of a police officer not below the rank of sub-inspector or b) upon a complaint made by a controller appointed under this Act or by any other person authorized by the controller.

The trial procedure of cyber tribunal shall follow chapter 23 of Criminal Procedure Code, 1893 (Trial Procedure by the Court of session) so far it is consistent. If the accused is absconded, tribunal can try the case in absentia. In this case tribunal has to circular an order in two Bangla news papers to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall have the same power, a Sessions Court empowered to apply in its original jurisdiction. Public prosecutor shall conduct the case on behalf of the Government. Tribunal shall conclude the trial within six months from the date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

4.4 Cyber Appellate Tribunal:

The Government shall establish one or more cyber appellate tribunal. The appellate tribunal shall be constituted by one chairman and two members appointed by the Government. To be appointed as a chairman of Cyber Appellate Tribunal, he must be either a former judge of the Supreme Court or existing judge of the Supreme Court or is eligible to be appointed as a judge of the Supreme Court. One of the two members of the tribunal shall be a retired District Judge or employed in the judicial service and the other member must be an experienced and skilled person in information and communication technology. They shall be appointed for 3-5 years. Cyber Appellate Tribunal shall have no original jurisdiction. It shall only hear and dispose of appeals from the order and judgment of the Cyber Tribunal and Sessions Court in appropriate cases. The decision of the appellate tribunal shall be final and it shall have the power to alter, amend, and annul the order and judgment of the cyber tribunal. The appellate tribunal shall follow the appellate procedure of High Court Division of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

4.5 Pornography Act 2012 and Child Pornography :

To protect the women and child and adult from sexual video, sexual harassment and also blackmailing and to prevent wide spread of video, MMS, picture through mobile or any way but mentioned the internet. In 8th March, 2012 this Act is enacted. In section 2 describe the definition of pornography.²⁰ In section 5 describe the investigation procedure and the other sections also describe the procedure of punishment and others such issues. But there has no any words which are clearly related with the cyber activities.²¹

But there has no other specific Acts and not have any other special guideline to prevent child cybercrime or actually child pornography at all. In short I understand that - Anti- pornography act (2012) has been enacted by the government of Bangladesh to make a restriction in the sharing and making pornography by the individuals as it brings a devastated result not only for the individual involved in it but also for the greater society. Section 4 stated that - Pornography production, storage, marketing, carry, supply, purchase, sell, hold or cannot be displayed.²²

Section 7- Investigation of any offense committed under this Act or the technical expert certified by the competent authority in the course of the offense has been committed to the government, autonomous, semi-autonomous organization in charge of the technical department of a license or authorization from the Government and private persons or any person or organization Technical competent institutions in charge of the accredited persons shall be treated as the opinions of experts from the comments received and it may be used as evidence in court.²³

Section 10- Offense committed under this Act shall be cognizable and non-bailable.²⁴

Section 11- Offense committed under this Act shall be in accordance with the procedure described in the Code of Criminal Procedure. Provided that the Government, by notification in the official Gazette, a special court or tribunal to judge crimes committed under this Act may delegate powers.²⁵ But it is also not sufficient to combat cybercrime. Because this Act deals with the only deals with the pornography.

4.6 Penal Code 1860:

²⁰ Section 2 of Pornography Act 2012

²¹ Section 5 of Pornography Act 2012

²² Section 4 of Pornography Act 2012

²³ Section 7 of Pornography Act 2012

²⁴ Section 10 of Pornography Act 2012

²⁵ Section 11 of Pornography Act 2012

Penal code 1860 describe the cybercrime involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject of penal laws of our country. The abuse of computers and also internet or cyber also given birth to a gamut of new age of crimes that are addressed by the special laws enacted to penalize these crimes.

For example ICT Act 2006 defines certain offence which does not cover by the Penal Code. On the basis of this law I think The Penal code of Bangladesh contains very few provisions regarding cyber-squatting. But in case of cybercrime like Hacking, Internet time thefts, Email bombing- there is nothing contained in our penal code. So it can be said that it is not possible for our government to control cybercrime by using some provisions of the penal code. To control cybercrime it is necessary to enact special law which only deals with cyber related matters.

4.7 Bangladesh Telecommunication Act 2001:

The Bangladesh Telecommunication Act 2001 has created a powerful regulatory authority in the telecommunication sector and section 53 of the Act gives the sector ample power to intercept the communication system to stop any sort of unwanted cyber incidents with the use of telecommunication tools in the country.²⁶ But this is also similar like the ICT Act, because there has also no more details about the cybercrime. It is the elaborate description about all types of telecommunications like mobile, internet, telephone, fax etc.

4.8 Cyber Crime Report :

The survey report titled Cybercrime Trend in Bangladesh-2022 says only around 7% of the victims received desired help after reporting to the police.

The Cybercrime Awareness Foundation published the report at the Crime Reporters' Association of Bangladesh auditorium in Dhaka on Saturday. Kazi Mustafiz, president of the foundation, chaired the event while East West University Senior Lecturer of law Monira Nazmi Jahan presented the findings.

The survey asked 18 questions to 199 victims from 15 February 2021 to 2 March 2022.

²⁶ Section 53 of Bangladesh Telecommunication Act 2001

According to the latest report, 53 out of 199 victims, or 26% of the victims, complained to the law enforcers – up by around 5% than 2021.

The 2021 report found around 22% of the cybercrime victims who filed complaints with police got positive outcomes.²⁷

The latest report shows the number of female complainants is comparatively less than that of male complainants. Among women victims, only 11.06% approached law enforcement agencies, while 45.73% were reluctant to take legal action.

The report found that around 21% of the victims did not take legal action to keep the matter secret. In addition, 17% of the victims did not take any action to protect their social image, 17% were afraid of harassment, and 17% thought that they would get no result from taking legal action.

However, 7% of the victims did not take any action because the accused person was influential. On the other hand, 2% of the victims did not feel the need to take action.

The report also found that 43.22% of the victims know about the laws related to cybercrime while the remaining 56.78% have no idea about that.

Most of the participants in the research were the victims of cyberbullying including receiving pornographic content, defamation threat, threats through social media, phone, messages etc.

This year's survey showed a slight increase in the number of victims of cyberbullying to 50.27% from 50.16% in the last report.

There has been an alarming increase in cybercrimes like social media and other online accounts hacking or information theft. In addition, the number of victims of fraud using social media and buying products online is also noticeable.

The report found that 23.79% of the participants were victims of online account hacking including social media. In the 2021 report, the rate was 28.31%.

However, in the last report, the incidence of spreading misinformation through social media was 16.31% which is 18.67% this year.

In the latest report, harassment by using photos or videos of sexual harassment incidents or intimate moments has increased at an alarming rate.

The rate of harassment using photos or videos of private moments or sexual harassment incidents was 7.69% last year, but it has increased to 9.34% this year. The incidence of harassment by using photoshopped images was 5.85% last year, which has increased to 6.93% in the new report.

²⁷ <https://www.tbsnews.net/bangladesh/55-cybercrime-victims-failed-police-survey-476406>

As per the report, about 15% of victims were defrauded while buying products online.

Most of the victims are 18-30 years old which is 80.90% of the total participants. Around 13% of the victims are under 18 years of age, 5.03% are aged 31-45 years and 0.50% are aged above 45 years.

Chapter-5

Challenges for Implementation or Combating CyberCrime

5.1 National Plan:

It is very difficult to make a new law. Because of, if we want to make a new law we have to run in the process, which is very hard procedure for us. First and for most important thing is that we have to make a national plan to combat that types of crime. The government should make a plan where all works together to address the threat of cybercrime. For that reason, I think which laws we have are not sufficient, actually these Acts are not made for only cyber related matters. To implement this sought of laws we have to follow some rules like:

- 5.1.1 **Understanding the problem:** Firstly, we have to realize the problem, actually the modern problem. Now a day all are totally connected with the internet and for that reason they are getting crime by the internet and they are same as normal criminals. So we have to find the types of offences and then we can get a decision. But in our laws I can't find any sections which define how to understand the problem.
- 5.1.2 **Partnerships and shared responsibility, individual crime:** Cybercrime is an individual type crime but sometimes it will be made by a group, but this is very rare. Whereas, individually we can't combat it, to implement it we have to work by a group or partnership work and receive an individual responsibility. Then we can reduce it. In our Acts it is clear that how to investigate and who has the power to investigate. But there has not mention the system how they work in this field.²⁸

²⁸ <<https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx> [last visited 21st September, 2016].>

- 5.1.3 **Focusing on prevention:** Our laws have no any sections which can elaborate the system of focusing on prevention. But we have to get target to prevent that crime forever. If we bound by the law to fixed the target for prevent it then this crime will be stopped.

5.2 Law Makers on the Basis of Cyber:

In our modern era or digitalization country has to make another body that is totally very intelligent on the field of cyber or internet. In our country we have no such individual body to make laws on the basis of internet. Natural intelligence is making laws. They aren't well known about the internet very clearly. Now that is the problem, that when they have not much idea about it then how they enact laws on this? Because they only see the problems but they won't know how to solve of these problems. And they make laws which are not suitable for that situation. So I think if we make bodies which are consisted with IT specialist, then we can receive an appropriate Act on this sector.

5.3 Law Ministry on the Basis of Cyber:

We have no any individual ministry on the basis of cyber related matters or on the basis of internet sector. But now a day it is a big problem in our society. Many people are committing such offences rapidly as like the natural offender. Because of we have no any guardian on this. If our government makes a ministry then we will be safe from the cyber criminals. Because this ministry is our guardian. And I think if we have a guardian then we can make laws on our demand and this ministry consists with the scholars.

5.4 Public Awareness about Cybercrime:

It is very important to inform to the people about all types of matter about cybercrime. If they are not well known about that matter clearly then they may commit such offence. If we through our eyes to that matter we can see that, today's we have no any awareness about the cybercrime. For that reason, we are committing such types of offence.

5.5 Internet Based Education:

Today's children are tomorrow's future. But in our educational system is based on books. We have to inform them about the cyber related issues by their lessons. Otherwise they will be committed cyber offence for their illiteracy on this sector. Bangladesh government should do this. But where are they? Just making laws are not the responsibility but also implementation is the right way to protect the society. So internet based education is the very important thing to avoid cybercrime.

5.6 Digital Security:

Our country has no any strong security, for that reason our system is hacked by many criminals in several times. If our security is hard then it won't be done anymore. We have also a Digital Nirapotta Ain 2018. But this Act also as like as ICT Act 2006. This Act is not sufficient to combat cybercrime. We should make a strongest security Act. Otherwise our country will be hampered day by day.

5.7 Investigational Power and Investigational System:

By our laws it is specified that at least a sub-inspector can investigate it. But if he is not intelligent about that sought of matter, then what will be done? It totally destroyed because of his illiteracy about cyber related matter. This investigational system is same as other crime also. Is the other crime and the cybercrime is same? No, never this is not same at all. So why the investigation procedure is same? I don't know. If the investigation invested to the scholars who are well known about the cybercrime. Then we can rely on it and we can receive a better investigation report. The investigation system is as like as other cases. But it is totally IT based crime and we have to follow the IT system and depend on it, otherwise we will miss the appropriate information. Perhaps in our country it will not be followed.

Chapter-6

Findings, Analysis, Recommendation & Conclusion

6.1 Introduction:

Conclusion means the finish of an event. Each research came to a similar conclusion. So I have also. This is a research on the basis of combating cybercrime. By this research I want to suggest to our government to enact the proper cyber law, making an individual and independent body to investigate in that matter only. I want to suggest for making a ministry also to coordinate the body on the demand. In present days there have a new communication system we can see and a dramatic changes we can see in the digital technology system. But the security system for using internet is not so strong. On the basis of this research I found that Bangladesh is under a serious cyber threat. Bangladesh is a digital developing country and the number of internet user's increase rapidly, but we have no anybody to control them. For that reason we can see the problems as like the stealing money from the bank, produce the obnoxious videos in the internet through the mobile or computer. All types of crime also held by the using internet, but we have not a proper body to handle it. In Bangladesh we can see a number of cybercrime have come under public attention in the last few years. One of this is a death threat to Sheikh Hasina, and then Leader of the Opposition. For this threat they are using emails, hacking of websites run by law enforcing agencies and defamation of private information of respected and popular individuals of the country are some of the examples of cybercrime in Bangladesh. In short it is clear that we have to make a law on it. And we have to make another body to enforce it.

6.2 Findings:

On the basis of my research I found some problems in chapter four. That:-

- Our Information and Communication Technology Act, 2006 is not sufficient for dealing to combat cybercrime.
- In this Information and Communication Technology Act, 2006 Act only some sections are dealing with the cybercrime, but it is not clear.
- Punishment is not appropriate for that sought of crime; which is mentioned in Information and Communication Technology Act, 2006.
- There is not mentioned the all cybercrime at all.
- It is the law of all types of communication system.
- To protect the cyber, government makes the Digital Nirapotta Ain 2008; but this is same as Information and Communication Technology Act, 2006. There is no any basic changes will be found.
- Digital Nirapotta Ain 2008 describe the what is lawful access and what is unlawful access. It is not so clear and it is very controversial.
- There have no any section that says about that how to combat cyber crime
- Pornography Act 2012 and Child Pornography also enacted for protect the cyber from the pornography.
- This Act won't cover the all sector of cybercrime. No one publish any porn in the internet; this is the process but where the solution?
- Our Penal Code never says about the cybercrime, but in section 13 describe the similar offences.
- Bangladesh Telecommunication Act 2001 is deals only cellular network. It is not so modern or not deals with cybercrime at all.

6.3 Critical Analysis:

It is rightly said that prevention is better than cure. It is always better to take certain precautions while operating the internet. As Bangladesh is a part of the world community and the country is emerging as an economic as well as political power in the South-Asian region with its GDP of no less than 6.5% over a couple of years, including 7.05% of the year 2016, and a cyber-revolution with the slogan of Digital Bangladesh, which is evident in her providing computer or Internet facilities across the country, including even the remote villages, there is every possibility of cyber-attacks on its cyber system involving financial sectors at any time. It may destroy not only the Internet environment but also the economic condition and development of the country as is evident from the recent Reserve Hacking of 80 billion US dollar of the Bangladesh Bank, the central bank of the country. All the economic, social and political atmosphere of the country, as addressed above, may turn vulnerable by means of such cybercriminal

activities that may happen in the country or outside the country. It is, therefore, high time the people of the country have been not only aware of the issue but also sincere in dealing with the Internet or computer arena. In this view one may keep in mind the followings:

1. Children should not give their identifying information such as their names, home addresses, school names, and phone numbers in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive. They should remember that people online might not be who they seem.
2. Parents should use content filtering software on their computers so that their child is protected from pornography, gambling, drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3. People should keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4. People should always use latest and update anti-virus software to guard against virus attacks.
5. People should never send credit card number to any site which is not secured.
6. People should not do panic if find something harmful. If there arises any immediate physical danger they should contact local police. Moreover, they should avoid getting into huge arguments online during chat and discussions with other users, and be careful about personal information about themselves online.
7. People should be cautious on meeting online introduced person. They should try to keep record of all communication for evidence and not edit it any way.
8. Big organizations should implement access control system using firewalls, which allow only authorized communications between internal and external network.
9. The use of password is most common for security of network system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.
10. System managers should track down the holes, bugs and weaknesses in the network before the intruders do.

6.4. Recommendations:

6.4.1 Policies Recommended for Prevention of Cyber Crime in Bangladesh:

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be brought into practical part so that the practices become easier to implement. Policies recommended are as follows:

- Integrated policies are required to ensure the effective benefits from the information system. The basic challenge and issue in the development of a cyber-society is the lack of financial and trained human resources.
- A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secured and free from cybercrime and within the reach of a common man.
- Promotion of research & development in ICT area and also in Human Resources to be a core part of the system.
- Up-to-date, common, and mutually supporting cyber laws should be there to fight with cybercrimes and protection of intellectual property rights towards the creation of a cyber-crime free information society.
- Adoption of ICT standards, regulation, and quality assurance is a necessity to foster high quality of services and productions that keep competition in place for the benefits of the communities within each country.
- High levels of awareness in each part of the society should be there in regard to information security and cybercrimes and increased exchange of information on information security and cybercrime at the regional and national levels should be there.
- Effective mechanisms should be there for the detection and prevention of cybercrimes and for improving protection against, detection of, and response to, cybercrimes, at the lower level itself.
- Conducting national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and private sector using different media is also a must.
- The government should educate and involve the media professionals, and then encourage them to increase public awareness.
- People should engage large private sector corporations and industry associations in the sponsorship of awareness programs.

- Stress should be laid on less developed countries on effective systems for protection against, detection of and responses to, cybercrime.
- People should promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.
- Law enforcement personnel must be trained and equipped in addressing high-tech crimes. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- People should use established network of knowledgeable personnel to ensure a timely and effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis.
- The government should welcome outsourcing initiatives to prepare a galaxy of virtual police officers and establish few cyber police stations across the country as soon as possible. These cybercrime fighters should be given specialized training home and abroad.
- Awareness raising, education, and technical support to prevent e-crime (anti-social behavior over the internet or via electronic devices) is essential, but without discouraging the development of e-commerce.

6.4.2 Recommended for the Prevention of Cyber Crime in Bangladesh:

Cyber-attacks could emerge as a major threat to the digital transformation of Bangladesh given the poor knowledge and lack of government initiatives to counter the growing problem, according to the study. Therefore, it is always better to take certain precaution while operating the net.

- 1) **Firewalls (network security system):** These are programs that protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom the user permits.
- 2) **Frequent password changing:** with the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep

passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.

- 3) Safe surfing:** Safe surfing involves keeping one's e-mail address private, not chatting on open systems, which do not have adequate protection methods, and visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimize the risk.
- 4) Frequent virus checks:** One should frequently check one's computer for viruses and worms. Also any external medium such as floppy disks and CD, ROMS should always be virus checked before running.
- 5) Email filters:** These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
- 6) Online photography:** Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- 7) Undergo:** Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
- 8) Credit Card security:** To guard against frauds one should never send credit card number to any site that is not secured.
- 9) Depravation in children:** Always keep a watch on the sites that children are accessing for the purpose of preventing any kind of harassment or depravation in children.

10) Secure the Program: It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

11) Watching Traffic: Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

12) Protecting Internal Network: Web servers running public sites must be physically separate and protected from internal corporate network.

13) Backup: Make Backups of Important Files and Folders to protect important files and records on computer if one's computer malfunctions or is destroyed by a successful attacker.

14) Off Internet: Disconnect from internet when not in use. Some other advises to be addressed while using the Internet or computers:

- Habitually download security protection update patches & keep your browser and operating system up to date.
- Disable file sharing on computers.
- Turn off the network during extended periods of non-use, etc.

- Check online account frequently and make sure all listed transactions are valid.
- Use a variety of passwords, not the same for all the accounts.
- Never respond to text messages from someone unknown.
- Avoid posting cell phone number online.
- Open email attachment carefully.

6.4.3 Recommendation:

First of all, I think it is very important to make a new sense of internet for all. We have to be aware about this. On the basis of this research I recommend some solutions; that:-

- Firstly, we have to realize the problem
- We have to make a law only on the basis of cybercrime
- An individual ministry is very important to take care of this law
- An individual and independent body has to make for implement this law. Who can exercise their power as like police or another law enforcing agencies?
- This body has to appoint scholars; who are well educated on the field of IT sector
- It is very important to make a cyber-forensics lab
- We want a cyber-store house
- If we make a system that no one can access internet without his/her NID number or Birth Certificate number without inputting in to the internet
- We have to establish an internet based education
- Public awareness is most important to implement this law

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

6.5 Conclusion:

In the evening it is very important to say that, without proper education about the internet, and then we cannot make a safe house of internet. To make a digital country it is very important to make a strong law on the basis of situation. If we follow that recommendation then we can find the solution at all. It is very important to think that all cybercrimes are like as civil crimes. We have to protect our country immediately.

BIBLIOGRAPHY

Books :

- 1) Ahmed DR. Zulfiqar, A Text Book On Cyber Law in Bangladesh
- 2) D.Rodney Ryder, Guide to Cyber Laws, 2nded. (Nagpur:Wadha & Company, 2005)
- 3) Kumar Vinod- Winning the Battle against Cyber Crime.
- 4) Mehta Dewang- Role of Police In Tackling Internet Crimes.
- 5) Duggal Pawan-The Internet: Legal Dimensions.
- 6) Monjur Kader: Criminology (Cyber Crime)
- 7) Internet History of Bangladesh, by Hamidur Rashid.
- 8) Cyber Crime and Bangladesh Perspective, By A.R.M Borhanuddin.
- 9) Computer Crimes: Cybercrime Information, Facts and Resources.
- 10) Insight to Cybercrime, by Nadia Khadam

List of Statutes:

- 1) The Information and Communication Technology Act, 2006
- 2) Digital Security Act 2016
- 3) The Penal Code, 1860 (Act No. XLV of 1860)
- 4) Bangladesh Telecommunication Act 20015.
- 5) Criminal Code of Procedure 18986.
- 6) Pornography Act 20127.
- 7) The National Information and Communication Technology (ICT) Policy (October,2002).

Journals:

- 1) Duggal Mr. Pavan,'Causes of Cyber', Intenational Journal of Computer Science and Information Security, Vol.3, No. 1(October, 2009).

2) Biswas Ripon Kumar, 'Cybercrimes need more attention,'

Tuesday, September 09, 2008.

Websites:

- <http://sufi-faruq.com/en/combating-cybercrime-a-bangladeshi-perspective-2/>.
- <https://www.tbsnews.net/bangladesh/55-cybercrime-victims-failed-police-survey-476406>
- <<https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx>[last visited 21st September, 2016].>