

RESEARCH MONOGRAPH
ON

CYBER CRIME TRIAL SYSTEM IN BANGLADESH: PROBLEMS AND PROSPECTS.

MD.ANISUR RAHMAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS(LL.M)

DEPARTMENT OF LAW
SONARGAON UNIVERSITY(SU)

5th JANUARY,2023

Title Page



RESEARCH MONOGRAPH

ON

CYBER CRIME TRIAL SYSTEM IN BANGLADESH: PROBLEMS AND PROSPECTS.

MD.ANISUR RAHMAN

ID. : LLM 2103024011

PROGRAM : MASTER OF LAWS (LL.M)

BATCH : LL.M-24

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS(LL.M)

DEPARTMENT OF LAW

SONARGAON UNIVERSITY(SU)

Declaration

I do hereby declare that the research monograph entitled, **"Cyber Crime trial System in Bangladesh: Problems & Prospects "** submitted to the Department of Law, Sonargaon University (SU), for the partial fulfilment of the degree of LL.M. All the materials presented for examination is my own work and has not been written for me, in whole or in part, by another person. I also undertake that any quotation or paraphrase from the published work of another person has duly been acknowledged in the work which I present for examination.

Md. Anisur Rahman
Roll No.: LLM 2103024011
Department of Law
Sonargaon University (SU)

Acknowledgement

At first I would like to thank Allah for his blessing and kindness, without her help it was quite impossible to complete the work. I am grateful and indebted to all, who have helped directly and indirectly to the preparation and finalization of my research paper.

At the very outset I would like to express my profound service of gratitude to my supervisor **Sharmin Jahan Runa,** Assistant Professor, Department of Law, Sonargaon University(SU). Without his inspiration, kind co-operation and guidance the work cannot be all completed. His co-operation was enthusiastic and motivating.

I would like to thank some of my friends who had been a great help. Finally, I am obliged to my family for their inspiration that helped me while working for this.

Name : Md. Anisur Rahman

Roll No. : LLM 2103024011

Department of Law

Sonargaon University (SU)

Abstract

Cyber and technology related crime is gradually increasing in Bangladesh. It is a significant issue in Bangladesh. But in Bangladesh the system of cyber crime trial should not be changed. In this research paper we find out the main problems of cyber crime trial system in Bangladesh and also analyze the main challenges to improve the cyber crime trial system in Bangladesh. The necessary data will be collected from primary and secondary sources. The secondary data will be collected from books, magazines, articles, research reports, official publications, theses, degree these Relevant and primary data will be collected by judges, defenders, litigants, members of legal committees, secretariat of law and justice. In addition, Cyber bullying is becoming a major concern for parents on the subject of their children using the internet as majority of students in Bangladesh have experienced being bullied or disturbed online or being bullied by the same person both online or offline. Moreover, cybercrime is becoming a threat to government itself. Due to lack of necessary legislation to tackle such type of crime, cyber criminals are almost in the safe side to commit such crime. In the Information and Communication Technology Act-2006 and ICT (Amendment) Act-2018 there are several clauses against cybercrime. But this Information and Communication Technology act is not the concrete one. By enacting this act, there is a chance to become safe side after committing crimes. So, considering these facts a comprehensive Cybercrime Protection Act should be imposed. This research work incorporates the recent trend and issues of cybercrime in Bangladesh especially focus on the area of Personal life, Workplace as well as Policy making Bodies or Thinkers. This research paper would help all relevant concerns and especially policy makers.

Key Words: Crime, Cybercrime, Trial, System, ICT, Digital forensic, Technology, Cyber Tribunal, Cyber Appellate Tribunal, Punishment, Investigation, System.

TABLE OF CONTENTS

Declaration i

Acknowledgements ii

Abstract iii

Contents ..... iv-v

List of Abbreviations vi

CHAPTER ONE : INTRODUCTION **1-5**

1.1 Background of the Study ……. 1

1.2 Statement of the Problem ……. 2

1.3 Research Questions …… 3

1.4 Research Objectives …… 3

1.5 Research Methodology …… 3

1.6 Literature Review …… 4

1.7 Research Scope & Limitation …….. 5

CHAPTER TWO : OVERVIEW OF THE CYBER CRIMES IN BANGLADESGH **6-13**

2.1 Introduction …….. 6

2.2 Definition of Cyber Crime …… 6

2.3 Nature of Cyber Crime …… 7

2.4 Classification of Cyber Crime …… 7-9

2.5 Characteristics of Cyber Crime …….. 9

2.6 Present situation of Bangladesh ……... 10

2.7 Cyber Crime in Bangladesh ……. 11-12

2.8 Bangladesh is not safe from Cyber Crime ……. 13

CHAPTER THREE : LEGAL FRAMEWORK ON CYBER CRIME **14-26**

3.1 Introduction 14
3.2 National framework on cyber crime 15
3.2.1. ICT Act,2006 15-17
3.2.2. Digital Security Act, 2018 17-20
3.2.3. The Penal Code,1860 21
3.2.4 The pornography Control Act, 2012 21
3.3 International framework on Cyber Crime 22-23
3.4 Responsible Institutions for Cyber Crime in Bangladesh 24
3.4.1. BTRC 24
3.4.2. Bangladesh Police 24-26

CHAPTER FOUR : PROSECUTION CYBER CRIME & ANALYSIS ON CYBER CRIME TRIAL SYSTEM **27-35**

4.1 Existing trial system on Cyber Crime in Bangladesh 27
4.1.1. Cyber Tribunal in Bangladesh 28
4.1.2. Cyber Appellate Tribunal in Bangladesh 28
4.2 Punishment for Cyber Crime in Bangladesh 28-31
4.3 Cases under ICT Law in Bangladesh 31-33
4.4 Challenges in Cyber Crime trial system in Bangladesh 34-35

CHAPTER FIVE : FINDINGS, RECOMMENDATIONS & CONCLUSION **36-39**

5.1 Findings of the Study 36-37
5.2 Recommendations 37
5.2.1. Legal perspective ..... 37 -38
5.2.2. Strategic perspective 38
5.2.3 Technical perspective 38-39
5.3 Conclusion 39
Bibliography 40-41

LIST OF ABBREVIATIONS

Abbreviation	Title
ACH	Automated Clearing House
ADC	Assistant Deputy Commissioner
Art.	Article
CID	Crime Investigation Department
CrPC	Code of Criminal Procedure
Dept.	Department
DIG	Deputy Inspector General
EFT	Electronic Funds Transfer
Govt.	Government
HCD	High Court Division
ICT	Information and Communication Technology
IGP	Inspector General of Police
IO	Investigation Officer
NSA	National Security Agency
PCA	Pornography Control Act
RAB	Rapid Action Battalion
Sec.	Section
UN	United Nations

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study:

Computer crime or cybercrime is a form of crime in which the Internet or computers are used as a means of committing crimes. When an online user accesses the Internet, personal information on his computer naturally brings valuable information into cyberspace that attracts cyber criminals. Furthermore, if cyber criminals have sufficiently capable computer systems, the inertia of the target of crime becomes almost weightless in cyberspace. The nature of visibility and accessibility within the IT environment allows motivated cyber criminals to detect criminal objectives and commit crimes from anywhere in the world. Any criminal activity that uses a computer as a tool, an objective or a means to perpetuate more crimes is part of cyber crime.[1] Cybercrime can be "illegal acts where the computer is a tool or a target or both".

Bangladesh is now moving forward with the goal of becoming digital Bangladesh within the 2021 vision with the specific goal of using e-government in all government agencies. Criminals use this technology to carry out new crimes and commit traditional crimes in new ways. They can commit these crimes with access to countless victims, anonymity and from anywhere in the world, making it difficult to identify and prosecute.[2]

Criminology tends to study all forms of crime that persist in society with discoveries of the causes of that particular crime and recommends prevention methods. Computer crime is no exception. But in recent times the nature and size of this crime has

[1] Tarun,2013"CyberCrime",LSI.p.l.accessedon,http://www.legalserviceindia.com/articles/cyber.htm

[2] Yar, M. (2005). The novelty of "cybercrime" An assessment in light of routine activity theory. European Society of Criminology, 2, 407-427.

changed dramatically in Bangladesh. It has become necessary to identify the Problems of Cyber crime trial System in Bangladesh.[3]

There is a sharp increase in cybercrime in Bangladesh and the law enforcement mechanism is finding it really difficult to handle these technical crimes in Bangladesh. Cybercrime has already become a constant concern in both the private and public sectors in Bangladesh. It has already been identified that especially financial institutions: private or public are the most threatening organization for cybercrime that reflects personal life at the same time.

1.2Statement of the Problem:

Bangladesh, despite being a third world country, has seen a technological revolution. A teenager from Bangladesh has easy access to computers and other devices. And so, they have enough opportunities to participate in piracy. Piracy has already become a serious problem in Bangladesh. Not only young people, even the mainstream media often engage in computer piracy and the dissemination of private information.[4]

New forms of cyber crime occur every day and if left unchecked, the situation of law and order will worsen.[5] The nature of cybercrime is changing in Bangladesh and needs to be identified so that new mechanisms can be introduced to maintain future public order situations. By changing crime patterns with the development of science and technology, the previous literature on this topic is becoming insufficient to provide accurate information and protection. Furthermore, most of the previous literature is written by academics who have no practical knowledge. Therefore, many books on cybercrime are found in different libraries; and mainly some aspects of the activities of the Cyber Tribunal and the Cyber Appellate Tribunal. But none of them contain adequate information on what Bangladesh should now know about cybercrime and the correct cybercrime trial system.

[3] https://www.academia.edu/13465468/CYBERCRIME_AND_ITS_IMPACT_IN_BANGLADESH_A_QUEST_FOR_NECESSARY_LEGISLATION

[4] http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/

[5] http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/

1.3 Research Questions:

(1) What are the compelling challenges in the cyber crime trial System in Bangladesh?

(2) What can be done to improve the cyber crime trial System in Bangladesh?

1.4 Research Objectives:

(1)To explore the cyber crime trial process in Bangladesh.
(2)To investigate the cyber crime legal framework in trail system
(3)To explore the nature of contemporary cyber crimes and it consequences in Information and Communication Technology world.
(4) To find out the main problems of cyber crime trial system in Bangladesh
(5) To analyze the main challenges to improve the cyber crime trial system in Bangladesh

1.5 Research Methodology:

Research Approach

Although the proposed study is mainly of a qualitative nature, both qualitative and quantitative approaches will be used for validity and reliability. In order to discover the Cybercrime Trial System in Bangladesh, an analytical approach study will be conducted.

Sources of Data

The necessary data will be collected from primary and secondary sources. The secondary data will be collected from books, magazines, articles, research reports, official publications, theses, degree theses, etc. Relevant and primary data will be collected by judges, defenders, litigants, members of legal committees, secretariat of

law and justice, division of the Ministry of Justice and Parliamentary Affairs, relevant laws for procedures and civil and criminal relations, monthly declarations and annual reports of the Supreme Court, the Legal Committee, the Ministry of Justice and the courts of district and session judges.

1.6 Literature Review:

Apart from these works, a list of other books, articles, documents, statutes, and journals on different aspects Cybercrime may be found but it is a matter or research but the truth is that as regards cyber crime trial system in Bangladesh: Problems and Prospects, no comprehensive evaluation has actually been made which includes all points theoretical and practical.

Cyber Crime means use of Computer Technology in Committing Crime. On the other hand Cyber Crime may be defined unlawful acts wherein the computer is either a tool or a target or both. In Bangladesh following types of cyber crime is happening: Cyber Hacking, Cyber Fraud, Cyber Pornography, Virus Introduction, Cyber Terrorism, Cyber Defamation and Disclosure of Confidentiality and Privacy. For doing this research monograph I have used some key words. Those are Digital Signature, Electronic, Electronic data inter-change, Electronic From, Electronic Record. Internet, Electronic Mail, Data message, Controller, Computer, Controller etc. In Bangladesh there are many laws for controlling crime. Those are ICT Act 2006,ICT Rules 2010,Pornography Control Act 2010,Information Rights Act 2009 and Bangladesh Telecommunication Act 2001.Among them I have discussed the problems and prospects of ICT Act 2006.

This research paper the quantitative and qualitative method to collect data. To find out about the cybercrime trial system in Bangladesh, I used an analytical approach methodology. It is true that the new multimedia technology represents an indisputable opportunity all over the world to promote and progress in human society. With this we must not forget that nothing is absolute in this universe, everything has its disadvantages or demerits. Some are applicable to the Internet and new technologies in

the age of communication convergence. This new Internet technology can be used to commit crimes or cause damage or injury to the company. A new generation of criminals seems to be destroying the computer, the computer system, the mobile phone with Internet connection, the wireless network, the Internet telephone system, the webcam and the like, which are applicable in electronic commerce, electronic governance, etc. Cyberspace has no specific jurisdiction; therefore, criminals can commit crimes from anywhere through the computer in the world without leaving evidence for control.

1.7 Research Scope & Limitation:

The present research work is to explore the cyber crime trial system in Bangladesh and to find out the problems and prospects of the ICT Act 2006. For that reason this research also find out cyber crime trial system in Bangladesh and the punishment for that related crimes and also find out the problems and challenges of cyber crime trial system in our country. This research have also given recommendation for the main challenges to improve the cyber crime trial system in Bangladesh.

The research has suffered certain limitation as below:

- The duration of the study was very short. More in dept investigation would have resulted better outputs.
- Lack of resources has hampered the study to some extent
- Access to information is very difficult. In most cases, concerned persons were very rigid to share adequate information.

CHAPTE TWO: OVERVIEW OF CYBER-CRIMES IN BANGLADESH

2.1 Introduction:

Bangladesh, despite being a third world country, has seen a technological revolution. A teenager from Bangladesh has easy access to computers and other devices. And so, they have enough opportunities to participate in piracy. Piracy has already become a big problem in Bangladesh. Young people are increasingly interested in emotional hacking. Not only young people, even the mainstream media often engage in computer piracy and the dissemination of private information.

2.2 Definition of Cyber Crime:

The term "cybernetic" derives from the term "cybernetic", which means the science of communication and control over the machine and man. Cyberspace is the new horizon controlled by an information and communication machine between human beings throughout the world. Therefore, crimes committed on machines or devices related to cyberspace or computer technology-related crimes should be treated as computer crimes.[6]

Professor S.T. Viswanathan has provided 3 possible definitions of cybercrime and these are the following: (a) any illegal action where a computer is a tool or an object of crime; in other words, any crime, the means or purpose of which is to influence the function of the computer. (b) Any incident associated with information technology in which a victim has suffered or could have suffered a loss and an author intentionally committed or could have made a profit. (c) Computer abuse is considered to be any

[6] Broadly speaking, cybercrime is an internet crime that includes piracy, terrorism, fraud, illegal gambling, cyber bullying, cyber theft, counterfeiting, virus flow, cyber porno.

illegal, unethical or unauthorized behaviour related to the automatic processing and transmission of data."[7]

2.3 Nature of Cyber Crime:

A cybercriminal can destroy websites and portals by hacking and planting viruses, performing online fraud by transferring funds from one corner of the world to another, gaining access to highly confidential and confidential information, causing harassment due to obscene emails or material threats, game taxes.[8] fraud, enjoy cyber pornography with children and commit countless crimes on the Internet.[9] It is said that no one is safe in the cyber world. Security is only for the present moment in which we are truly safe. With the increasing use of the Internet, cybercrime would affect all of us, directly or indirectly.[10]

2.4 Classification of Cyber Crime:

a. There are certain offences which affect **the personality of individuals** can be defined as:

- Harassment via E- Mails
- Cyber-Stalking:
- Dissemination of Obscene Material
- Defamation
- Hacking
- Cracking
- E-Mail Spoofing
- SMS Spoofing
- Carding
- Cheating & Fraud

[7] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary,2001,p.81.

[8] M. Abul Hasanat, 'Cyber Crime: An ill.going Techno Culture'. Journal of Law, Vol. i, no.01 (June 2003), p.15

[9] Translation from Bangla to English; Dr.Zulfiqar Ahmed; *Bangladesher Cyber Ain ar Tatta o Bislation*;(Muhit Publication, February ,2014);P:377

[10] *Ibid,* p.141.

- Child Pornography

b. 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:

- Intellectual Property Crimes
- Cyber Squatting
- Cyber Vandalism
- Hacking Computer System
- Transmitting Virus
- Internet Time Thefts
- Cyber Trespass

c. Cybercrimes against Government:

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities.[11] It includes:

- Cyber Terrorism
- Cyber Warfare
- Distribution of pirated software
- Possession of Unauthorized Information

[11] Cyber Crime Prevention, 12th February 2015, from http://memorv.loc.gov/cgi

d.Cyber-crimes 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:

- Child Pornography
- Cyber Trafficking
- Online Gambling
- Financial Crimes
- Forgery[12]

2.5 Characteristics of Cyber Crime:

Taking into account the above factors, we can classify computer crimes. The classification of cybercrime is a very complex task because it is a new criminal show with a growing and growing phenomenon.

There are several ways to classify cybercrime. One way is to classify into three main categories (1) The computer is the target and the victim. (2) The computer is secondary to another crime. (3) The crimes associated with the prevalence of computers that are also called computer crimes. . For example, in hacking, computer theft, computer blackmail, etc., the computer is the target. Sometimes, the computer is not the essential factor for the commission of crimes, but it is a factor to facilitate the crime is fast and new procedures with rapid communications. Here the computer is secondary to other crimes, such as cyber pornography, harassment, illegal banking transactions and others. Another category are the crimes associated with the prevalence of computers, p. software piracy, forgery, etc.

Don Parker has identified four forms of computer abuse, namely: (1) the computer could serve as a victim of crime; (2) the computer could constitute the environment in which a crime was committed; (3) the computer could provide the means by which a

[12] Vijayashankar.Na (Naavi).6 february 2003.Essentials of Cyber Laws for IT Professionals present at sairam Engineering College on February 18.2003 during the seminar on cryptography. http//www.naavi.o9rg/cl editorial_03/cl_eng_htm

crime is committed or (4) the computer could be used symbolically to intimidate, deceive or defraud the victims.

Another way to classify cybercrime is (1) Violations against the confidentiality, integrity and availability of data and the computer system, which include illegal access, illegal interception, data interference, system interference, illegal devices, etc. . (2) Computer related infringements, p. For example counterfeiting, sabotage, cyber bullying, etc. (3) Offense related to the content, p. Child pornography, infringement of intellectual property rights, etc.

2.6 Present situation of Bangladesh

There are not enough laws in the Asian nation that could penalize cyber criminals. In the Bangladesh court there is a law called "Bangladesh Information and Communication Act 2006" (amended in 2018). During this law, section 56 (1) declared a sentence of ten years in prison with or without a fine.

The sixty-eight article of the aforementioned act established the formation of a special court called "Cyber Court". The World Health Organization could consider these forms of cyber crime, however, it is to stop or penalize criminals..

Due to the inadequacy of qualified specialists who help the court, it is virtually impossible for him to choose to follow the trail by punishing the criminal. There is only one IT magistrate in the city of Dhaka established pursuant to article eighty-two of the aforementioned law. However, this judiciary has not rewarded any social control for any criminal. Apart from this, until the establishment of the cyber judiciary within the district court, the chosen session has the knowledge to judge a crime reasonably under section seventy-four of the aforementioned act.[13]

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

In the Asian nation there is a legal authority called BTRC which acts as a watchdog in computer security, however, it is to satisfy its guarantees. It is the authority to conduct mobile courts with the assistance of alternative government agencies for the swift process of such a reasonable crime. The development of science and ICT depends on the growth of the telecommunications sector. This sector remains below development attributable to the lack of liberation and free competition.[14]

The impact of cybercrime is not scary. Bangladesh, due to monetary transactions, has not been fully optimized online. acquires the tools and infrastructure to prevent, warn and process them.8 But our government has not yet realized the fact. Web services provided through the native space network may be subject to similar attacks and intrusions by hackers when the level of protection is insufficient.[15] Currently, every day in Bangladesh, some people send malicious e-mails to completely different foreign commissions and alternative VIPs that generally cause a big problem for the police and also for the government.

2.7 Cyber crime in Bangladesh:

Life is a mixture of good and evil. This is the internet Despite all the good things it does, cyberspace also has its dark sides. However, unlike conventional communities, there are no police officers patrolling the information highway, leaving it open to everything from Trojan horses and cyber bullying viruses to counterfeit brands and cyber terrorism. . A few months earlier, a group of people had violated the Bangladesh quick-acting battalion website. When this incident was published in the media, almost all government institutions were afraid. Nobody wants to believe it. Subsequently, RAB arrested some people and they are now in prison. One of the main hackers on the RAB website, Shahee Mirza, said that no one should use their computer skills acquired in criminal activities such as piracy of important government or private sites. After hearing your statement, many cybercrime experts in Bangladesh are afraid.

[14] The Financial Express (10 January 2008)

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

Although the 2006 Information and Communication Technologies (ICT) law covers many of the legal aspects of cybercrime repression, it has not been effectively implemented since ratification.[16]

According to experts, the main reason for the inefficiency of the law is the lack of legal support and social and public awareness of cyber crime. Cybercriminal analysts 10 Point out that although pornography is not considered illegal worldwide, in Bangladesh it is one of the main cybercrimes. There is already evidence of the existence of pornographic websites hosted illegally with local content. In Bangladesh, young people increasingly use cybercafés as meeting places. According to newspaper reports, these cafes carry out various types of antisocial activities in the name of web browsing.[17]To browse the Internet, there are separate booths for couples where their intimate moments are secretly recorded. These images are available later on the Internet. According to section 57 of the ICT Act of 2006, a person convicted of uploading vulgar and obscene content on the website is punished with a 10-year prison sentence and a maximum Tk sentence, but nobody cares What in our country does not it's still us. Have an effective IT court to resolve this issue. That is why it is very easy for cyber criminals in Bangladesh to get rid of punishment.

2.8 Bangladesh is not safe from cyber crime:

Cyber crime has increased rapidly in Bangladesh in recent years. The number of cyber crime cases has increased almost 200 times. Most cases were filed under section 57 of the Information and Communication Technology (Amendment) Act of 2018. However, recent cyber court statistics show that this law is used to harass people with cases Without a base, 73% of women are subject to cybercrime.[18] Crime in Bangladesh Cyber pornography refers to the representation of sexual material on the

[16] http://www.ittefaq.com.bd/issues/2008/07/19/news0019.htm
[17] http://www.thedailystar.net/newDesign/archive.php? Last visit 20th march 2018
[18] http://en.prothomalo.com/bangladesh/news/122235/Cybercrimes-on-the-rise-due-to-section-57

web.[19] Criminals often kidnap or annoy a girl, capture the incident via a webcam or mobile phone and stream the video online.

We have several laws to manage cybercrime and between these two promulgations are important for practical purposes: the Information and Communication Technology Act, 2006 (ICTA) and the Porn Control Act, 2012 (PCA). Computer pornography can be searched in section 8 of the APC and also in section 57 of the ICT act. It will be extremely difficult to elaborate an act of transformation if the transformed image / video does not enter into the meaning of pornography. The acts of cyber bullying will probably continue to be immune from legal proceedings, since these laws do not specifically define them and our first instance judges will be reluctant to condemn a person for acts not defined as crimes.

[19] https://bdnews24.com/bangladesh/2017/03/09/73-percent-women-subject-to-cyber-crime-in-bangladesh

CHAPTER THREE : LEGAL FRAMEWORK ON CYBER CRIME

4.1 Introduction:

In the current era of rapid growth. Information technology covers all areas of life around the world. These technological developments have made it possible to move from paper transactions to paperless transactions. Now we are creating a new creation, new standards of speed, efficiency and precision in communication, which have become key tools to stimulate innovation, creativity and increase overall productivity. Computers are widely used to store confidential data of a political, social, economic or personal nature that offer enormous benefits to society. The rapid development of the Internet and information technology around the world has led to the growth of new forms of translational crimes, in particular linked to the Internet. These crimes have virtually no limits and can affect any country in the world. Therefore, it is necessary to raise awareness and implement the necessary legislation in all countries for the prevention of computer crimes.[20] Globally, commerce and Internet-based communications and information technology cross territorial boundaries, thus creating a new area of human activity and undermining the feasibility and legitimacy of the application of laws based on geographical boundaries.[21] This new limit, which consists of screens and passwords, separates the "cyber world" from the "real world" of atoms. The police and the territorial authorities judge this new environment as deeply threatening.

[20] http://dohatec-ca.com.bd/DohatecCA/ICTAct.jsp

[21] http://www.business-standard.com/article/opinion/cyber-security-no-longer-a-governmental-responsibility-115100500137_1.html accessed 01 September, 2016

4.2 National framework on cyber crime:

Following are the laws for controlling cyber crime in Bangladesh:

1. . Digital Security Act,2018
2. Information and Communication Technology Act,2006
3. Information and Communication Technology Rules, 2010.
4. Pornography Control Act, 2012.
5. Information Rights Act, 2009
6. Bangladesh Telecommunication Act, 2001.

4.2.1 Information and Communication Technology Act-2006:

The ICT Preamble Act of 2006 stated that, an act to provide legal transactions performed electronically due to the lack of a legal framework. At present, many legal provisions (such as the law on evidence, 1872, the penal code, 1860. the law on the evidence of bank books, 1891, etc.) recognize paper documents and documents with the signatures of the parties and them make it admissible as evidence in various disputes Electronic commerce eliminates the need for such paper transactions and, as such, electronic transactions are often not recognized in court, which delays the growth of electronic commerce.

The ICT Silent Characteristics Act, 2006, was illustrated by the Final Report of the Legal Commission to implement the following purpose Incorporates provisions of both model laws

(a) facilitate electronic communications through reliable electronic records;

(b) facilitate e-commerce, eliminate barriers to e-commerce resulting from uncertainties about writing and signing requirements and promote the development of the legal and commercial infrastructure necessary to implement secure e-commerce

(c) facilitate the electronic transmission of documents with government agencies and

legal companies and promote efficient delivery of government services
(d) to minimize the incidence of counterfeit electronic documents, intentional and unintentional alteration of documents and fraud in electronic commerce and other electronic transactions
(e) promote public trust in the integrity and reliability of electronic registers and electronic commerce and promote the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence on any electronic medium.[22]

The Information and Communication Technology Act (ICT) of 2006 also aims to establish the legal framework to guarantee legal sanctity for all electronic records and other activities performed electronically. The law establishes that, unless otherwise agreed, the acceptance of the contract can be expressed by electronic means of communication and that has legal validity and enforceability

Cyber Tribunal:

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 on Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal.[23]
Cyber tribunal shall take a case for trial –

a) 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 Sessions)** so far it is consistent. If the accused is absconded, tribunal can try the case in absentia. In this case tribunal has to

[22] http://www.lc.gov.bd/reports/47.pdf accessed 01 September, 2016
[23] Ibid, S. 68 (2)

circular an order in two *bangla* newspaper to appear the accused on a specified date.13 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.[24]

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.[25] 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 Davison of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

[24] Zulfiquar Ahmed, pp. 150-152
[25] Ibid, S. 82 (3)

4.2.2Digital Security Act,2018:

Digital Security Act 2018 replaces The Information and Technology Act,2006.(ICT) Telecom and ICT Minister Mustafa Jabbar placed the proposed law before the House, which was sent to the parliamentary standing committee on the ministry concerned for scrutinizing it. The committee had also been asked to submit a report to parliament within four weeks.[26]

Objectives:

- "One of the main objectives of the proposed law is to ensure the country's security from digital crimes and ensure security of people's lives and assets," the minister said while placing the bill.

Background:

- Digital Security Act has formulated to combat growing cyber crimes.
- Journalists have been demanding to repeal of section 57 of ICT Act 2006.

Addition:

- Both bail able and non-bail able offences are included in the draft
- The draft was approved keeping a provision for revoking sections 54, 55, 56, 57 and 66 of the ICT act, and the cases already filed under section 57 will continue.
- Arrest without warrant by police.[27]

Section analysis:

[26] See, for example, Mafuz Anam, "Commentary: 'Analogue Law' for 'Digital Bangladesh'", 31 January 2018, The Daily Star. Available at: http://www.thedailystar.net/commentary/commentary-analogue-law-digital-bangladesh-1527565.

[27] [27] Ibid, S. 56 (3)

- **Section 4** of the draft Act illustrates the jurisdiction of the Act.
- **Section 5** says about constitution of a Digital Security Agency.
- **Section 13** of the Act illustrates the Power of the DG of Digital Security Agency
- **Section- 17** Uses digital media to intimidate people (threaten) or causes damage to the State. Imprisonment for 14 years or Tk-1 crore fine or both.
- **Section 57** deals with defamation, hurting religious sentiments, causing deterioration of law and order and instigating against any person or organization through publishing or transmitting any material in websites or in electronic form. It stipulates maximum 14 years in prison for the offences. Now, the draft of Digital Security Act-2018 splits these offences into four separate sections with punishment ranging from 3-10 years' term.The Digital Security Bill-2018 splits these offences into four separate sections (21, 25, 28 and 29) with punishment ranging from three to 10 years' jail term. In 2017 alone, at least 25 journalists and several hundred bloggers and Face book users were prosecuted under Section 57.
- **Section 21** says anyone spreading negative propaganda against the Liberation War or the Father of the Nation, using digital devices or instigates to do so, will risk being sentenced up to 14 years' jail or a fine of up to Tk 1 crore or both. He or she will face up to life sentence or Tk 3 crore fine or both for committing the offence for the second time, it said.
- **Section -25** A person may face up to 3 years in jail or Tk 3 lakh fine or both.A person will face up to 5 years in jail or Tk 10 Lakh or both for committing the offence for second time, it said.

- **Section 28** says a person may face up to 7 years in jail or Tk 10 lakh fine or both if he or she is found to have deliberately publishes or broadcasts something in the website or in electronic form or get it done to hurt one's religious sentiment and values.A person will face up to 10 years in jail or Tk 20 Lakh or both for committing the offence for the second time.
- **Section- 29** A person may face maximum 3 years in jail or Tk 5 lakh fine or both if he or she commits offence stipulated in section 499 (DEFAMATION)

of the Penal Code through website or in electronic form. He or she will face up to 5 years in jail or Tk 10 Lakh fine or both for committing the offence for the second time, it said.

- **Section-30** Using electronic devices for unauthorized transactions for bank and insurance.5 years in jail or tk 5 lakh fine or both.
- **Section -32** On the charge of spying if he or she illegally enters the offices of government, semi-government and autonomous bodies to gather information and uses electronic device to record something secretly.A person may face up to 14 years in jail or Tk 20 lakh fine or both.The provision an updated version of section 3 of the Official Secrecy Act of 1923 on spying. Journalists and law experts fear that abuse of the proposed law would hinder rights ensured by the Right to Information Act 2009.
- **Section -34** For Hacking- A person may face up to 14 years in jail or Tk 1 core or both .
- **As per section 43 of the draft,** a police official can search or arrest anyone without any warrant issued by a court. If a police officer believes that an offence under the act has been committed in a certain place or is being committed, or there is a possibility of crimes, or there is a possibility of destroying evidence, he or she can search the place or any person present there. The officer can arrest any person if he or she suspects that the person has committed or is committing crimes. In such a case, the officer has to submit a report to the court after carrying out the search, it added.[28]

The government has approved the draft to tackle digital crimes. But the apprehension is that the proposed law could be used to suppress freedom of expression in the country. Mentioning the Act as a threat to freedom of speech, expression and the safety of the citizens, the Transparency International Bangladesh (TIB) has called for amendment to the draft law. Clearly, the government has taken a significant step to ensure digital security in Bangladesh. However, the proposed law exposes various loopholes. Many journalists and right activists believe that the government may use

[28] Ibid, S. 82 (3)

some of its controversial provisions as a sword rather than a shield to control their voices and activities. But the government strongly believes that the proposed law will be used as a shield for the innocent party and a sword for bad people.

4.2.3The Penal Code, 1860:

Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to penal laws of Bangladesh. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the special laws enacted to penalize these crimes.[29]

ICT Act 2006 defines certain offences which are not covered by the Penal Code. In this regard, I would like to say that the Penal Code 1860 is not effective enough in dealing with cybercrime in Bangladesh.

4.2.4The Pornography Control Act, 2012:

The Parliament has enacted a law by the title of Pornography Control Act, 2012. The preamble says this Act has been enacted to prevent deterioration of moral and ethical values of the society. Information technology with its immense benefits has got some disadvantages as well if it is used by mischief people with criminal intention. It has been seen in our country that video clips, MMS etc of sexual intercourse or behavior relating to sexual activities have been recorded on camera by a section of people and then used to blackmail, cheat, defame girls and women.[30]

The Act has been enacted upon those who produce pornography using a child, man or woman, taking their still pictures, video or film with or without their consent and print, distribute and publish such materials or sell, supply or exhibit child pornography.207 This Act convicts a person if any pornography is being transmitted through the internet, website, mobile phone, or any other electronic device and the punishment is

[29] The penal Code 1860,S.32
[30] Preamble, The Pornography Control Act, 2012

prescribed of imprisonment for up to 5 years and fine up to BDT. 5,00,000.Government may constitute Tribunal which is yet to be established for trial of offences under the Act and No Rules have been made by the Government as of now.

4.3 International framework on cyber crime:

The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th May 2000.the preamble of this Act states its objective to legalize e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000. So that they may regulate and control the affairs of the cyber world in ineffective manner The Information Technology Act deals with the various cyber crimes in chapters IX& XI. The important sections are Ss. 43,65,66,67. Section 43 in particular deals with the un authorized access, un authorized downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Core by way of remedy. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.[31]

Here I like to present a list of cyber laws existing in different parts of the world:

[31] For the sake of convenience the readers are requested to read sections 43, 65, 66,67 of the Information Technology Act.

India:

- Information Technology Act, 2000
- Karnataka Cyber Cafe Regulations
- Gujarat Information technology Rules, 2004.
- IN Domain Name Dispute Resolution Policy (INDRP)
- Rules for Information Technology Act 2000
- Semiconductor Intergrated Circuits Layout Design Act 2000
- Semiconductor Integrated Circuits Layout-Design Rules, 2001
- IN Domain Name Registration Policy
- The Information Technology (Amendment) Bill, 2006
- MOVED: Req: Indian Telegraph Rules, 1951

USA:

- THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998
- Deleting Online Predators Act of 2006
- Adam Walsh Child Protection and Safety Act, 2006
- CAN-SPAM Act 2003
- FTC's Guidelines for Internet Advertising
- Uniform Domain Name Dispute Resolution Policy
- Computer Fraud and Abuse Act
- Federal Trademark Act 1946 (The Lanham Act)

Europe:

- Data Protection Act, 1998
- The Electronic Commerce (EC Directive) Regulations 2002
- Regulation of Investigatory Powers Act 2000
- European Model EDI Agreement Legal Provisions
- UK Electronic Communications Act 2000
- UK: Copyright and Rights in Databases Regulations
- Council of Europe's Convention on Cybercrime 2001
- The British Code of Advertising, Sales Promotion ...
- UK: The Consumer Protection Regulations 2000

- UK: NOMINET Dispute Resolution Service Policy (Ver. 2)

Pakistan:

- Electronic Crimes Act 2004 (Sec 1 to 18)
- Electronic Crimes Act 2004 (Sec 19 to 36)

4.4 Responsiable Institutions for cyber crime in Bangladesh:

4.4.1Bangladesh Telecommunication Regulatory Commission(BTRC):

BTRC has created a special cell to fight cybercrime. The 11 members of the Bangladesh Computer Security Incident Response Team (BD-CSIRT) will monitor malicious activities on the Web and respond to any setbacks.

BTRC states that this initiative will ensure information security and at the same time play an effective role in blocking fraudulent online activities. Giasuddin Ahmed, vice president of the committee, leads the team of commission members, representatives of mobile operators, Internet service providers, PSTN, International Internet Gateway and Internet cafes. BD-CSIRT has published a website, a telephone number or e-mail to check the computer crime. Telephone: 02-7162277 or add 444; Fax: 02-9556677, Email: contact@csirt.gov.bd

Anyone can write or call their complaint at that address. On the other hand, a person can file FIR against cyber criminals to get remedies at any Bangladesh police station.[32]

4.4.2 Bangladesh Police:

In today's world, the information system and network security have become a correct problem because information has become increasingly important to everyone, as

[32] Translation from Bangla to English; Dr.Zulfiqar Ahmed; *Bangladesher Cyber Ain ar Tatta o Bislation*;(Muhit Publication, February ,2014);P:377

information protects and develops human life every day. Understanding the essential need for security, all developing countries have taken steps to address the problem; on the other hand, developing countries are far from being able to guarantee these rights. Threats to the information society were emerging at the content level. However, information security cannot be achieved only with technology. To respond to the threats of the network and create a secure information society, comprehensive prevention measures and implementation measures are needed.

In Bangladesh, the Internet user is increasing rapidly. Bangladesh police recently planned to set up a special unit to contain cybercrime. The issue has become more urgent since an email was sent to the Bangla Daily Protom Alo, throwing a life-threatening threat to the president of the Awami League and to the current Prime Minister Sheikh Hasina on August 23, 2004. A another email to police headquarters on 25 August. , treating the opposition leader and the last prime minister, Begum Khaleda Zia, his son Tarique Rahman and the legislators of the Nationalist Party of Bangladesh. The police department took e-mails seriously and decided to set up a cybercrime control unit, which will be the country's first cybercrime police unit. Two young men, a private university student and a software engineer, were arrested in connection with the email threat.

According to reports, the first two said they sent the mail for fun. Since there is no national IT infrastructure, a surveillance or security system has not yet been developed in Bangladesh. While the threat of cybercrime looms in the country with the rapid increase in the use of the Internet and modern technologies, the speakers of a regional seminar have underlined the need to issue an Internet crime law to combat these crimes.[33] They also called for global cooperation to fight cybercrime, as it is not limited by borders. They suggested formulating an internet crime law as soon as possible and providing adequate training for law enforcement to combat such crimes. The Bangladesh police, in association with the federal police of Australia, organized a three-day computer crime seminar which started at the Sheraton Dhaka Hotel with the

[33] Kabir. Ahmed and Chowdhery. Shuvra(2015) Media and cyber Laws In Bangladesh. 2nd edn. Dhaka, Bangladesh: sufi prokashoni

aim of sharing experiences and promoting cooperation in the fight against cyber crime. Experts from Australia, Hong Kong, Sri Lanka, Nepal and the host country participate in the seminar. Seminar opening, provisional government. LGRD consultant Anwarul Iqbql said cybercrime is not limited by borders, as criminals exploit the technology available on the market today. As a transnational crime, cybercrime is a global problem with global impact. He added that it is necessary for developing countries to fight cybercrime, although their cost is a burden to them.

He cited various types of cybercrime, such as computer piracy, counterfeit credit cards and child pornography, stating that it is difficult for law enforcement to handle such crimes. He also stressed the need for cooperation between countries in this regard. To date, our ability to fight cybercrime is inadequate, said the former Interior Secretary, adding that Bangladesh is trying to formulate a cybercrime law and that the bill is already in place. Australian high commissioner Douglas Foskett said cybercrime has become a topic of concern worldwide. Given that Bangladesh is witnessing rapid growth in Internet usage, must prepare to face the threat, he said, the Australian High-Tech Crime Center offers assistance to several countries in this regard.

The additional inspector general and the director of the national police reform program (PRP) NBK Tripura said that cyber crime and technology are on the rise.[34] Citing the news of the law on the Internet, he said that cybercrime has grown to overcome illegal drug sales worldwide and analysts estimate that online fraud will generate $ 105 billion in 2007. It is also estimated that the cost of data loss due to malicious activity.

[34] Bangladesh Police set up Cyber Crime Unit, 8th February 2015,fromteletechblog.blegspot.com/2013/05/cyber-crime-cyber-security-and.html.

CHAPTER FOUR: PROSECUTION CYBER CRIME AND ANALYSIS ON CYBER CRIME TRIAL SYSTEM

4.1 Existing trial system on cyber crime in Bangladesh:

4.1.1.Cyber Tribunal in Bangladesh: According to section 68 of the "Information and Communication Technology Act 2006" the government may establish one or more tribunals to make speedy and effective trial for the crimes committed under this Act and the government will determine the Local Jurisdiction of that tribunal.

Judge: According to section 68(2) the government shall appoint a session judge or an additional session judge for the cyber tribunal in consultation with the Supreme Court.

The Trial System: In two terms the cyber tribunal tries the cyber crime. They are:

- With the report of police who is not below rank of Sub-inspector.
- With the report of any other person approved by the 'controller' or any other person authorized by the controller mentioned in the ICT Act 2006.

The cyber Tribunal shall follow the consistent and relevant part of chapter 23(of trials before court of sessions) of the criminal procedure code 1898 to try the cyber criminals. If the accused person is being escaped the tribunal order him to appear in court by publishing advertisement in two national Bangla news paper and can continue the trial in absence of the accused person. The Tribunal can order for re-investigation with the application of either party or by *suompto*.

To try cyber criminals the Tribunal shall follow the criminal procedure so far as possible and apply them. To exercise the Original Jurisdiction how much power the session court holds here in the Cyber Tribunal he holds the same power. The public prosecutor(PP) conducts the case on behalf of the government.

The Tribunal shall end the trial within 6 months from the date of allegation. If the Tribunals thinks necessary he may extends it for 3 months. The Judgment shall be pronounced within 10 days after the ending of prosecution. The Tribunal may extend the pronouncement of judgment for 10 days.

4.1.2.Cyber Appellate Tribunal in Bangladesh:

According to section 82 the government may establish one or more Cyber Appellate Tribunal. This appellate tribunal shall be consisted by a chairman and two members appointed by the government. A person who was or is a justice of Supreme Court or is qualified to be appointed as the justice of Supreme Court shall be the chairman of that appellate tribunal. One of the two members of the tribunal is a person who is retired or still working in the judicial service as a district judge and the other one who is expert and have enough experience in information and communication technology. They shall be appointed for 3-5 years.

The Trial System: The Cyber Appellate Tribunal won't have any Original Jurisdiction. The jurisdiction of this tribunal is to hear and decide the appeals against the judgment cyber tribunal. The cyber appellate tribunal holds power to retain, revoke, cancel, alter, amend the verdict of cyber tribunal and the decision of cyber appellate tribunal shall be final.
If the Cyber Appellate Tribunal is not established according to this law the appeal from the cyber tribunal shall lie to the high court division of the Supreme Court.

Special Branch: Like other countries to identify and prevent cyber crime the government established a squad of special branch of police consisting IT Experts. They keep their vigilant eyes on the computer user and suspected cyber criminals. The branch of police, CID is also engaged with their assistance to prevent this type of crime in Bangladesh.

4.2Punishment for Cyber Crime in Bangladesh:

The following activities are regarded as offence according to section-54, such as; If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,-

a) Accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so[35]

b) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) Damages or causes to be damaged willingly to any computer, computer system or computer network. data, computer database or any other programmers residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies of causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network, in contravention of the provisions of this Act, rules or regulations made there under;

h) for the purpose of advertisement of goods and services, generates or causes generation of spasm or sends unwanted electronic mails without any permission of the originator or subscriber;

[35] The information and Communication Technology Act, 2006, S.82(3)

i) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.
If any person commits any of the aforesaid offence, 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.

The ICT Act describe punishment for tampering with computer source code is if any person intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network. when the computer source code is required to be kept or maintained by any law for time being in force, then this activity of his will be regarded as offence.[36] Whoever commits this type of offence shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to Taka three lakhs, or with both.

The ICT Act describe punishment for hacking with computer system is if any person, intentionally 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.[37] or cause damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him; then such activity shall be treated as hacking offence.[38]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

The ICT Act describe punishment for disclosure of confidentiality and privacy is no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register,

[36] Ibid., s. 55
[37] bid., s. 56(1)
[38] Ibid., s. 56(2)

correspondence, information, document or other material to any other person shall be regarded as an offence[39]
Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or with time which may extend to Taka two lakhs, or with both.[40]

The ICT Act describe punishment for using computer for committing an offence is whosoever knowingly assists committing crimes under this Act, using any computer, e-mail or computer network, resource or system shall be regarded as an offence.
Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or with time which may extend to Taka two lakhs, or with both.

The ICT Act describe punishment for using computer for committing an offence is whosoever knowingly assists committing crimes under this Act, using any computer, e-mail or computer network, resource or system shall be regarded as an offence.51 Whoever aids committing these types of offence he shall be punishable with the punishment provided for the core offence.

The ICT Act describe punishment for Offences committed by companies etc then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.

4.3 Cases under ICT Law in Bangladesh:

Case 1. In June 2003, Cyber pirates hacked into the Internet account of Barisal DC office marking the first cybercrime in the Barisal region. The computer hacking

[39] Ibid., s. 63
[40] Ibid., s. 66

incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Telegraph and Telephone Board (BTTB), which is the internet service provider for the DC office. The hackers, who somehow got hold of the password of the account, accessed it from several places in town including an IT firm, residences of an ADC and a joint secretary, and a Pharmaceutical company.[41]

Case 2. An e-mail message was sent to Bengali daily Prothom Alo, issuing a life threat to Awami League president and Leader of Opposition Sheikh Hasina on August 23, 2004. Another mail was sent to the police headquarters Aug 25, threatening Prime Minister Khaleda Zia, her son Tarique Rahman and Bangladesh Nationalist Party (BNP) lawmakers. The police department took the mails seriously and decided to set up a cybercrime control unit, which will be the country's first policing unit against cybercrime. Two young men, a private university student and a software engineer, were arrested in connection with the e-mail threatening the prime minister and another youth for threatening Sheikh Hasina.[42]

Case 3. In 2008 a pretty hacker of Bangladesh named Shahee Mirza hacked the RAB's website. Moreover, he confessed to police that not only RAB's website but also other national govt., non govt. and international sites had been hacked by him for a long time. Totally he hacked 21 websites together with Army's website. So it is clear to us that the cyberspace of Bangladesh is not secured as there is no nationwide computer infrastructure,[43] no watchdog or security system has yet been developed in Bangladesh.

Case 4. 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

[41] International Journal of Law and Legal Jurisprudence Studies: ISSN:2348-8212: Volume 2 Issue 4
[42] Daily Prothom alo_23 August, 2004
[43] Hasan, Mahdy, *Cybercrime: Implementation Must to Achieve Vision 2021*, 30 June 2012, The Daily Star, Page 6

Facebook account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were destroyed.

Case 5. On 15/02/2012 a group of alleged Bangladeshi hackers named „Black Hat Hackers hacked more than 25000 Indian websites which included important sites such as the website of the Border Security Forces (BSF). Propaganda activities are also considered as cyber-crimes in some instances. Propaganda is information which is biased and misleading in nature used to promote or publicize a particular political cause or ideology. It creates agitation and panic among the public.

Case 6. Bangladesh war crimes tribunal chief quits over Skype scandal: The head of a Bangladeshi tribunal which has been dealing with crimes committed during Bangladesh's 1971 war of independence against Pakistan resigned on 10th December 2012 amid controversy over the leak of his Skype conversation with an expatriate Bangladeshi legal expert. International Crimes Tribunal-1 chairman Justice Md Nizamul Huq mentioned "personal reasons" for his resignation, then State Minister for Law and Justice Quamrul Islam told The Daily Star 10th December 2012 evening.[44] His resignation would not hamper the proceedings at the tribunal set up in 2010 to try the cases over crimes against humanity, said sources concerned. Although 2006 Information and Communications Technology (ICT) Act covers many of the legal aspects to prosecute cybercrime, but it has not been effectively implemented since its ratification.[45]

4.4Challenges in cyber crime trial system in Bangladesh:

The investigation and trial procedure of cyber crime presents a number of challenges for law enforcement agencies. Proper legislation is the foundation for the investigation and prosecution of cybercrime. However, lawmakers must continuously respond to

[44] http://shatgombuj.com/bangladesh-war-crimes-tribunal-chief-quits-over-skype-scandal 2/416; Asia News Network *Tuesday 11th December, 2012*

[45] http://www.pipilika.com/site_ajax_calls/show_details/46719/en/new_window

Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.

Historically, the introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s – the first unauthorized access to computer networks occurred shortly afterwards. Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when these systems were used to copy software products. It takes time to update national criminal law to prosecute new forms of online cybercrime. Indeed, some countries have not yet finished with this adjustment process. Offences that have been criminalized under national criminal law need to be reviewed and updated. For example, digital information must have equivalent status as traditional signatures and printouts. Without the integration of cybercrime related offences, violations cannot be prosecuted.

The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates. Many countries are working hard to catch up with legislative adjustments. In general, the adjustment process has three steps: adjustment to national law, identification of gaps in the penal code, and drafting of new legislation.

Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to penal laws of a country. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the special laws enacted to penalize these crimes. For example, in Banlgadesh Tatha O Jogajog Projukty Ain 2006 “Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 defines certain offences which does not cover by the Penal

Code. And so it can be said that the Penal Code, 1860 is not effective enough in dealing with cybercrimes.

The causes of this may be that no Cyber Tribunal and Cyber Appellate Tribunal have been formed by the government yet. Moreover as per the provisions of the ICT Act a good number of other procedural and structural hurdles also exist which are as follows:

Firstly, in tribunal procedure, judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the opportunity to be assisted by the ICT expert. But is it possible to give the verdict on the basis of another's knowledge? The reality in our country is that so far no initiative is taken by the government to train up the judges for acquiring the minimum technological knowledge required for **Secondly**, a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer)[46] regarding the cybercrimes. Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. So, it is not possible for such a police officer to make a proper investigation into such matters. Moreover, it may result in a snag to justice.

Thirdly, the government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of those proposed tribunals.[47] Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state.

Proper execution of statutes ensures the rule of law. Circumstances say that inadequate execution of the ICT Act, 2006 is one of the root causes for the increasing cybercrimes

[46] Sec:82(2)(3), ICT Act, 2016.
[47] Sec:82(4), Ibid

in Bangladesh. The solution of those aforementioned problems demands that the state must take nippy steps along with logistic and financial assistance.

CHAPTER FIVE : FINDINGS, RECOMMENDATIONS AND CONCLUSION

5.1 Findings of the Study:

There are not enough laws in Bangladesh which may punish the cyber criminals. In Bangladesh court there is a law named "The Bangladesh Information & Communication Law 2006" (As amended in 2019) . In this law section 56(1) has declared the penalty of 10 years imprisonment with or without fine.

Section 68 of the said act has declared the formation of a special tribunal named "Cyber Tribunal". Who is may take cognizance of such kinds of Cyber Crime but it has yet to prevent or punish the criminals. It has not yet reward any kind of punishment.

Due to the scarcity of trained specialist assisting the court it has become very much impossible for the judge to trace the crime as well as the criminal and to punish him. There is only a cyber tribunal in Dhaka City established under section 82 of the said act. This tribunal has not yet reward any punishment to any criminal. Out of this till to the establishment of Cyber Tribunal in the district court the Session Judge has the cognizance to trial such kind of crime under section 74 of the said act.

In Bangladesh there is a statutory authority named BTRC which perform as a watchdog in cyber protection but it is yet to fulfill its promises. It has the authority to conduct mobile courts with the help of other government organs for the speedy trial of such kind of crime.

The offences of the Bangladesh Information & Communication Technology Act 2006 are non-cognizable in nature under section 76(2). The victim has to file an allegation to the law enforcing agencies to get remedy. This is the main weakness of the said act.

In the time of enactment of the said act it was said in section 68 that a special tribunal named Cyber Tribunal will be established in every district of Bangladesh. But till now only a tribunal has established in Dhaka City.

Because of the dependency of technology specialist and well trained lawyer and judges the disposal of Cyber cases are rare. To remove such kind of pendency of cases judges, lawyer and specialist should be well trained.

The Bangladesh police have a special branch named "Anti-cyber Crime Department" headed by the Deputy Commissioner of Police to protect e-mail fraud, treat by e-mail, defamation or publishing of unauthorized pictures. But the department is yet to fulfill the public demand due to the scarcity of well trained man power. A case cannot be started due to the non visibility of the plaintiff. There is no scope for the state to take liabilities as being a plaintiff.

The Cyber Tribunal has not yet reward any punishment to any criminal. Due to this the criminals are insisting to occur crimes thinking that they will not be punished. This is one of the main weaknesses of the implementation of the Bangladesh Information & Communication Technology Act 2006.

5.2 Recommendations:

The results of this study led the authors to recommend a holistic approach to cybercrime treatment. The proposed holistic and collaborative approaches include three categories, namely: legal, strategic and technical perspectives for predicting, preventing, identifying and responding to computer crimes.

5.2.1 Legal perspective

i. A separate Cybercrime Protection Act should be enacted.

ii. The Government of Bangladesh should have cybercrime laws for dealing with cybercrime and there should be collaborations of different stakeholders (i.e. within organization, national wide and worldwide).

iii. There should be forensic bureau (competent in IT security) investigations/collection of digital cybercrimes evidences.

iv. High penalties should be enforced for cybercrime committed and for those who do not report the incident of cybercrime.

Training and awareness to citizens, organizations, the Government and public in general regarding the collection of digital forensics evidences; and how to report cybercrime.

5.2.2Strategic perspective

i.A comprehensive induction programs should be developed for all the concerns of ICT as pilot basis.

ii. The Government should revise the National ICT policy to accommodate new ICT developments in the industry.

iii. The organizations/Government should have Internet usage and security policies in specific

iv. Standards and procedures should be enacted with regard to usage of information systems in cyberspace.

v. Training and certifications in cyber security, information systems assurance, information systems security and other related risks management certifications or professional. The education system curricula should be reviewed to incorporate training in the field of information systems security and cyber security.

5.2.3Technical perspective

i.Special trained wing of police to combat cyber crime should be established. The rise of cyber crime insists the law enforcers to work as global police rather than regional or national police only.

ii. Cyber crime units can be established. Bearing in mind the present situation of using Internet and increasing cyber crime in Bangladesh, Government can also commence such types of agencies. The significance of such Units is that these will be able to perform multidimensional actions like advancing the Internet infrastructure, maintaining the ISPs, fixing the Internet using charges, preventing the cyber threats etc.

iii. Observe Group should be established. These groups can be one of the vital constituents for developing Bangladesh as an advanced country especially in Internet technology.

5.3 Conclusion:

Prevention is always better than cure. Computer crime is increasing day by day. As a result, we can be victims of any cyber attack at any time. We should take precautionary measures, as well as punitive measures against cybercrime. To be fruitful, the legislator, the Ministry of Information Technology, together with IT professionals and the media, must work together. Young generations must be aware of cyber crime. In addition to monitoring and controlling cybercrime, the Bangladesh cyber security incident response team (BD-CSIRT) must take punitive measures against criminals and, in some cases, BD-CSIRT must act directly against the people involved to perform harmful activities against students, society, state, political and religious beliefs using telephones, computers and other collateral devices. The Digital Security Act of 2018 strengthens the hand of Bangladesh-CERT to adopt emergency measures against cybercrime activities. In addition to the National Digital Security Agency (NDSA), the formation of the National Digital Security Council (NDSC), regional and international initiatives make us optimistic because the Bangladesh cyberspace is an area of secure communication in the coming days. There is also a need to bring changes in the Information Technology (ICT) Act to make it more effective to cyber crime trial system.

BIBLIOGRAPHY

Primary Sources:

Statutes:

The Criminal Procedure Code, 1898.

The Convention on Cyber Crime, 2001.

Digital Security Act,2018

The Evidence Act, 1872.

The Information and Communication Technology Act (ICT), 2006.

The Penal Code, 1860.

The Pornography Control Act, 2012:

The United Nations Commission on International Trade Law (UNCITRAL), 1996.

Secondary Sources:

Books :

Abdul Halim& N. E. Siddiki, The Legal System of Bangladesh after Separation, 1st ed., (Dhaka: University Publications, 2008).

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

Paranjape, N.V., Criminology and Penology, Central Law Publications, Allahabad, 2009

Yar, M., The novelty of "cybercrime": An Assessment in Light of Routine Activity Theory, European Society of Criminology, 2005, page 407-427

Zulfiquar Ahmed, A Text Book on Cyber Law in Bangladesh, 1st ed.,(Dhaka: National Law Book Company, 2009).

Online Journals:

Ashiquddin Mohammad Maruf, Md. Rabiul Islam, Babul Ahmed. ‗Emerging cyber crime in Bangladesh: In Quest of Ejective Legal Remedies' The Northern University Journal of Law, Vol..i, no. 1 (2010), p.01

M. Abul Hasanat, ‗Cyber Crime: An ill.going Techno Culture‗. Journal of Law, Vol.i, no.01 (June 2003), p.15

In Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408

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

R. E. Okonigene, and B. Adekanle, "Cybercrime in Nigeria", Business Intelligence Journal. Vol.3.No.1,pp.93-98, 2010.

M. Abul Hasanat, 'Cyber Crime: An Ill-going Techno - Culture', Journal of Law, Vol. no.1 (June 2003).

Joe Thomas, 'Cybercrime: A revolution in terrorism and criminal behawor created change in the criminal justice system‗. 21 July 2006

Online Books:

Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime

B.Magalla, The New Era of Cyberspace: Their Protection, Prevention and Detection

Charney, Computer Crime: Law Enforcement‟s Shift from a Corporeal Environment to the Intang ible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41.

Hayden, Cybercrime‟s impact on Information security, Cybercrime and Security, IA-3, page 3. Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18

Jones, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005

Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, Seymour/Goodman, page 225

Wallsten, Regulation and Internet Use in Developing Countries, 2002, page 2.

Website links:

Http://www.wrlawfirm.com/blog/2007/09/second-life-second-jurisprudence.html

Http://www.rediff.com/news/serach/2003/feb/18crime.htm last visit 20th march 2018

Http://www.thedailystar.net/newdesign/archive.php? Last visit 20th march 2018

Http://www.ittefaq.com.bd/issues/2008/07/19/news0019.htm

Https://krazytech.com/technical-papers/cyber-crime last visited 23th march 2018

Http://en.prothomalo.com/bangladesh/news/122235/cybercrimes-on-the-rise-due-to-Section-57

http://www.techterms.com/definition/cybercrime.

http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism.html?cat=37.

M. E. Kabay, 'Salami fraud' (*Network World Security Newsletter),* 24 July 2002, http://www.networkworld.com/newsletters/sec/2002/01467137.html.