

“Critical Analysis on the Cyber Crime and Cyber Security in Bangladesh”

THE DISSERTATION SUBMITTED TO DAFFODIL INTERNATIONAL
UNIVERSITY IN PARTIAL FULLFILMENT OF THE REQUIREMENT
FOR THE AWARD OF THE DEGREE

Master of laws

2018

Md.Abdus Salam
DIU/LL.M



Faculty of Humanities and Social Sciences

Daffodil International University

Dhaka, Bangladesh.

2018

**THIS RESEARCH MONOGRAPH IS DEDICATED
TO
MY FAMILY**

DECLARATION

I am **Md. Abdus Salam** student of LL.M (Final) hereby solemnly declare that, the presented work has been performed by me and has been submitted in the fulfilment of the requirement for the degree of Master of laws; LL.M (Final)

I declare that thesis has been prepared by me and has not previously been submitted to any other university/ organization for any academic qualification/certificate/diploma degree.

This work presented my original work and it's not submitted before.

.....

Md. Abdus Salam

ID: 181-38-238

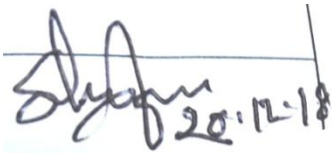
Department of law

Daffodil International University

CERTIFICATION

This is to certify that the thesis on “Critical Analysis on the Cyber Crime and Cyber Security in Bangladesh” is done by me in the partial fulfillment of the requirement for the degree of LL.M (Final) from Daffodil International University of Bangladesh. The thesis has been carried out under my guidance and is a record of this research which is carried out successfully.

It is further certified that, no part of dissertation has been submitted elsewhere for any Degree or Diploma.



.....
S. M. Saiful Hoque
(Supervisor)
Assistant Professor
Department of law
Daffodil International University

.....
Md. Raiduzzaman

Head of the department
Department of law
Daffodil International University

ACKNOWLEDGEMENT

Firstly, I offer millions of heartfelt thanks to Almighty ALLAH, who has given me strength to complete of this Research Monograph successfully.

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

I also take the opportunity to express my grateful to my honorable teacher **Md. Abu Saleh and Head of the law department, Mr.Md. Riaduzzaman** for his scholastic guidance, untiring interest, constructive criticism and creative suggestion throughout this research.

Also gratefulness goes to my respect teacher **Dr. Mizanur Rahman**, Professor of law, University of Dhaka and former Chairman of the National Human Rights Commission, Bangladesh.

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

IV

List of Abbreviation

BLT-Bangladesh Law Times

BCR: The Bangladesh Case Reports
NCR: National Crime Records Bureau
NGO: Non-governmental organization
HCD : High Court Division
ICT: Information and Communication Technology
ICTA : Information and Communication Technology Act
IT : Information Technology
ITA: Information Technology Act
MMS: Multimedia Messaging Service
PC: Penal Code
PCA : Phonograph Control Act
SMS : Short Message Service
SNWs : Social Networks
UK : United Kingdom
US : United States
EU : European Union
DSA: Digital Security Act
BTA: Bangladesh Telecommunication Act
ASEAN: The Association of Southeast Asian Nations
APEC: The Ministers and leaders of the Asia Pacific Economic Cooperation
INTERPOL: Interpol International Criminal Police Organization
OECD: The Organization for Economic Cooperation and Development

Table of Contents

Declaration.....	II
Certification.....	III
Acknowledgement.....	IV
List of Abbreviation.....	V-VI

Chapter I: Introductory chapter

1.1 Introduction.....	1
1.2 Problem statement.....	2
1.3 Rational of the study.....	2-3
1.4 Research question or Hypothesis.....	3
1.5 Research Objectives.....	4
1.6 Literature Review.....	4-5
1.7 Research Gap.....	6
1.8 Methodology.....	6

Chapter II: Concept of cyber crime

2.1 Definition of cyber crime	7-8
2.3 Historical Background of cyber crime.....	8-9
2.4 Nature of Cyber Crime	9
2.5 Classification of Cyber Crime.....	10-11
2.6 Characteristics of Cyber Crime.....	13-14

Chapter III: Legal Approach cyber crime prevention in Bangladesh

3.1 National legislation Protecting Cyber crime.....	15-16
3.1.1 Information and Communication Technology Act, 2006.....	16-17
3.1.2 Digital Security Act 2016.....	16-17
3.1.3 Pornography Act 2012 and Child Pornography.....	17-18
3.1.4 Penal Code 1860.....	18
3.1.5 Bangladesh Telecommunication Act 2001.....	18

Chapter IV : International legislation Protecting Cyber crime

4 .1 The United Nation.....19

4.2 The European Union.....20

4. 3 The Council of Europe.....20

4 .4 ASEAN.....20

4 .5 APEC.....21

4.6 Organization of American States.....21

4. 7 International Criminal Police Organization (Interpol).....21-22

4. 8 The Organization for Economic Cooperation and Development (OECD).....23

4.9 Treaties & International Agreements on Cyber Crime.....23

4.9.1 United Nations Convention against Transnational Organized Crime (2000).....23

4.9.2 Convention on the Rights of the Child (1989).....23

4.9.3 Optional Protocol to the Convention on the Rights of the Child (2001).....23

4.10 Digital Security Act legal Provision.....23

Chapter V: Challenges for Implementation or Combating Cyber Crime

5.1 National Plan.....24

5.1.1 Understanding the problem.....24

5.1.2 Partnerships and shared responsibility; individual crime.....24

5.1.3 Focusing on prevention.....25

5.1.4 Balancing security freedom and privacy.....25

5.2 Law Makers on the Basis of Cyber.....25

5.3 Law Ministry on the Basis of Cyber.....	25
5.4 Public Awareness about Cybercrime.....	26
5.5 Internet Based Education.....	26
5.6 Digital Security.....	26
5.7 Investigational Power and Investigational System.....	27
Chapter VI : Comparative case study	
6.1 Cyber crime in different countries.....	28-29
6.2 Cyber crime related Case.....	29
Chapter VII : Findings and conclusion	
7.1 Findings.....	30
7.2 Conclusion.....	31
Bibliography.....	32-33

Chapter I

Introductory chapter

1.1 Introduction

Internet is a very well known word however it started out in our us of a in 1996 on 4th June. This is a system of speak to every other and also the whole thing can do by way of net in the ones days. Internet is a mix of hierarchical systems, like IP addresses and routing. The actual time period “Internet” became subsequently described in 1995 through Federal Networking Council. It is a brief time period that “Internet” but it's miles a big group of millions of computer systems are linked by using phones or computer systems. No one manage the net, because of this the cybercrime is growing. Cybercrime can extensively be defined as a criminal hobby involving an records generation in fracture, together with illegal get admission to.

In short cybercrime is “Offences that are committed towards an person or institution of individuals with a criminal reason to intentionally harm the reputation of the sufferer or purpose physical or mental harm or loss to the sufferer at once or indirectly and additionally occasionally certain to suicide the use of present day telecommunication networks consisting of internet (chat rooms, emails, be aware forums or companies, social media, with the aid of sending junk mail) and cellular cellphone (SMS/MMS). Great improvement of the net is World Wide Web. This is the navigator of the internet. Bangladesh is a third world USA, it started her digital revolution. At that time the borders of this crime aren't binding, it spreads in worldwide market without difficulty.

It may be very clean to get entry to any computers via the usage of net, because we haven't any sturdy machine to forestall all and sundry. Now we are baby in the sector of internet and for that we have to control on get admission to internet. Bangladesh has no any unique law on the premise of internet, for that reason cybercrime is growing hastily. No you could forestall it. If we make a specific regulation and an unbiased frame who are professional in this, then we can consider the secure house of cyber.

This work gives a brief review of cyber-crime, explains why people are concerned in cyber-crime, look at those concerned and the reasons for their involvement, we might examine how excellent to hit upon a crook mail and in conclusion, proffer pointers that would help in checking the increasing price of cyber-crimes and criminals. These courses offer fashionable outlines as well as precise techniques for imposing cyber protection.

1.2 Problem Statement

The internet creates unlimited opportunities for business, social and other human sports. But with cybercrime the Internet introduces its very own unusual dangers. What are the hazard cybercrime and cyber safety threats poses to Bangladesh. The worldwide village presently information an growing crook conduct. News of cybercriminal sports maintain to fill the pages of the newspaper, it's miles central to worldwide data and has emerge as a global hassle. There is now and again a place wherein in computers and internet centers are found that cases of crime are not recorder .

If we make a frame like police or any other regulation imposing businesses only for the safety of this sector and if we keep a approach like- “every body who desires to get admission to internet, he/she have to hold a rule, then we are able to make a internet for entice the wrongdoer effortlessly.

Cyber crimes are described as one of the fastest developing criminal sports on the earth. He repeated the fact that it covers a massive range of unlawful pastime inclusive of economic scams, pc hacking, downloading of pornographic pics from the internet, virus attacks, stalking and growing web sites that sell hatred.

In latest time, younger students inside the tertiary engage in forgery of all kinds ranging from false admission paper to high school charges receipts, certificate racketeering and exam malpractice this is, gaining access to useful information all through examinations through the handset and other electronic devices .

1.3 Rationale of the study

Information plays critical role for an man or woman, cooperate area as well as for nation and united states of america. Bangladesh has emerged as a favourite among cybercriminals, mainly hackers and other malicious customers who use the net to dedicate crimes and due to inadequate rules and regulations privacy of facts is easily breached.

2. The observe goes to help in identifying specific modes by which cybercrime has been unfold the world over in addition to vast editions which may be used to stumble on and save you our society to combat with cybercrime.

2. To recognize rising cyber safety mechanism and various tasks taken through worldwide and countrywide groups so that destiny path can be traced in the direction of the improvement of enhance methodologies.

This studies makes a contribution to the experimental literature on the psychology of cyber criminals by extending preceding work on integrity. Another wonderful contribution of this studies is the perception it gives into accounting for anonymity when performing psychological research related to cyber crime.

1.4 Research questions

The study then attempts to answer the following questions:

1. How are Bangladesh anti-graft agencies tackling cybercrime and cyber security threats?
2. How effective and efficient are the efforts of the security agencies in combating cybercrime and ensuring cyber security in Bangladesh?
3. What can be done to improve the state of cybercrime and cyber security in Bangladesh?
4. What are the methods of dealing with cybercrime and how we are able to deliver a safe atmosphere in the vital space?
5. How can cyber security and cyber resilience be managed in the global supply chain and how does this differ from other supply chain risks?

1.5 Research objectives

The preferred goal is to offer information and evaluation which lawmakers, policy makers and law enforcement groups in Bangladesh can use so you can create crook definitions which can be great from sociological and technological perspectives of cybercrime and cyber safety.

The precise goals are as follows:

1. The most important purpose of this take a look at is to examine the reputes of cybercrimes and felony reforms in Bangladesh.
2. To take a look at and look at the quantity to which Bangladesh felony tips take a look at cyber laws development.
3. To study the volume of adequacy of the newly surpassed crook framework to limit cybercrimes in Bangladesh.
4. To understand informal, sociological and technological reasons of cybercrime and cyber safety in Bangladesh.
5. To assessment the techniques adopted with the useful resource of Bangladesh law enforcement agencies and cyber protection stakeholders in combating cybercrime and ensuring cyber protection.

1.6 Literature Review

This is a Studies which primarily based on, “Combating Cyber Crime in Bangladesh on basis of Laws and Policies”. Many men define the Cybercrime and manage, based on their revel in. Many people define, “what is cybercrime?” But I expect some materials are missing in their studies, that is, “Have any specific frame to manipulate it? I expect their definition isn't clean on the idea of this question”. Now an afternoon's many instances are filled at the idea of cybercrime. Sufi Faruq Ibne Abubakar, most effective one person; who write in this topic nice in his article. He stated that, “The idea of a Digital Bangladesh is welcomed by using the IT experts and the overall mass. To gasoline this notion the authorities need to deliver due significance to the trouble of cybercrime. Otherwise, like many other tremendous responsibilities this could fall on its face. It is a matter of desire that the “National Information and Information Technology Guidelines 2009” has protected

Cybercrime as an time table. To make this a achievement the Ministry of Information Technology, together with the IT specialists and the media should come ahead.”

In Bangladesh angle we've got a regulation, primarily based on cybercrime is ICT Act 2006. But this isn't always sufficient to lessen cybercrime. We must a frame which can manipulate it. There are many loopholes in our Acts. Now an afternoon's any person can inter within the internet

verywithout difficulty, but if we've got a body for control the field of internet and make some hard policies for get entry to net, then we are able to reduce the illegal activities in that area.

Dr. Amos Nudge, In his paper, he outlined foremost things. Firstly is that the government has the function and duty of ensuring that there's an good enough felony and exercise surroundings (rules, legal guidelines, requirements, policies are available and enforcement mechanism) to allow comfy and safe cyber transaction.

John Buena, Information Communication Technology (ICT) is unregulated in Bangladesh. It is actual for instance that, while one decides to unfold pc viruses maliciously, he cannot be prosecuted in Tanzania, the cause being that we do now not have law in vicinity to control or deal with that problem.

The Act offers with the law regarding Digital Contracts, Digital Property, and Digital Rights Any violation of those laws constitutes a criminal offense. Life imprisonment and nice up to rupees ten laths may be given for positive lessons of cybercrimes. Compensation up to rupees five cores can be given to affected humans if harm is performed to the pc, computer system or laptop community by the introduction of virus, denial of offerings and many others. The Act in particular deals with certain offences, which may be known as Cyber Crimes¹.

1.7 Research Gap

Research on the basis of specific topic is very big thing to do. Four months is not sufficient for research in a topic. Perhaps, I will try to invent a new thing on a short time. But there have no many books on that topic. There have not much journal to make this research and also very hard to make public opinion on that topic. Victims aren't sharing their problem frankly. We haven't much law on the basis of this project. Overall there are lots of limitations for this research on this field.

1.8 Methodology

This analysis is a qualitative and also quantitative basis. I also include the journals, Laws, reports, statistics, and also opinion of many specialists. This study used both primary and secondary data. Data from primary source was collected directly by the means of interview by the researcher. And Data from Secondary source was collected from different libraries, Bangladesh Communication Regulatory Authority and at the Bangladesh Law Reform Commission.

¹https://www.academia.edu/14184668/CRITICAL_ANALYSIS_ON_THE_STATUS_OF_CYBER_CRIMES_AND_LEGAL_REFORMS_IN_TANZANIA?fbclid=IwAR2hz4n-3sp1bVXftnaPFrxFxr1Yq1PEm6gjZ

Firstly, I want to find the problems. For using internet what types of problem will arise. I want to find the crimes which are related with the internet. Then I find the Acts which are related with that such of crimes. I should take the specialist opinion that the laws are sufficient or not for cybercrime and cybersecurity.

Chapter II

Concept of cyber crime

1.1 Definition of cyber crime

Along with the Phenomenal increase of the Internet has come the boom of cyber-crime opportunities . As a end result of speedy adoption of the Internet globally, computer crimes include no longer most effective hacking and cracking, however now additionally include extortion, toddler pornography, cash laundering, fraud, software pirating, and company espionage, to name some . Cyber crime is the deadliest epidemic confronting our planet within the millennium.

Broadly said, ‘ cyber crime’ may be said to be an act of commission or omission, committed on or thru or with assist of or related with, the Internet, whether or now not at once or indirectly, which Is prohibited with the aid of any regulation and for which punishment, economic and corporal is supplied . But the existing penal or crook laws are incapable to take action short to the fast revolutions in net and pc network technology.

The results of crimes devoted over the internet reach farther than conventional techniques of committing crimes due to the fact there aren't any geographical border restrictions.² Since cyber crime is an unbounded crime, without boundary lines crime. Computer crimes are hard to resolve due to the absence of geographical borders and the inherent potential to unexpectedly switch and manipulate facts immediately. Further complicating cyber-crime enforcement is the region of criminal jurisdiction.

Today, computers have an effect on all aspects our lives, from clinical treatment to air site visitors manipulate, on line banking and digital messages (“e mail”). The Internet presents tremendous benefits to society, consisting of the capacity to speak with others real-time, get right of entry to a library of statistics and transmit statistics immediately with out leaving domestic³.

Crime is greater or much less acknowledged to every person on his personal stand factor, whilst cyber is almost indistinct in meaning to the same. So if every person makes use of the prefix ‘cyber’ we surely mean, he's taking approximately something is doing online or there has positive networking machine. Actually anything associated with Internet falls under the cyber class.⁴The time period cyber crime is a misnomer. This term has nowhere been described in any statute Act exceeded or enacted by means of the Bangladesh Parliament.

³ Explanatory Memorandum, pp. 1-4.

⁴ M. Abul Hasanat, ‘cyber crime: an Ill- going Techno- culture’, journal of law, Vol, I, no 1 (June 2003), p, 15

2.2 Historical Background of cyber crime

Cyber Crime has had a short but tremendously eventful records. Apart from being an exciting have a look at by using itself, watching the records of cyber crime could also provide the individual and society the opportunity to keep away from the mistakes made within the past. Appropriate action can also be taken in the destiny. The first recorded cyber crime passed off within the year 1820! That isn't sudden considering the fact that the abacus, that's thought to be the earliest shape of a pc, has been around considering that 3500 B.C. In India, Japan and China. The era of present day computer systems, however, started out with the analytical engine of Charles Babbage.⁵

A textile producer in France named Joseph-Marie Jacquard changed into hindered to just accept new generation inside the weaving of unique fabrics via conventional employees of loom textile on 1820. This is the primary recorded cyber crime in global! And the modern age cyber crime is originated in new technique.

In the Nineteen Eighties organizations which include CompuServe, Prodigy, and AOL began to emerge. These were commercial carriers who could price a monthly rate to customers in the event that they desired to get admission to their "network". In the Nineteen Eighties the fee to dial into CompuServe turned into \$25 in keeping with hour (Wall, 2001). Users selected to connect through those agencies due to ease of use. There become no configuring; inserting a disk and jogging a application might have the person "stressed" In the early Nineties the costs for dial up internet decreased to \$25 consistent with month for unlimited get entry to. The decline in cost made it possible for greater online criminals to emerge in the anonymous on-line community.⁶

In 1990 and 1991 customers started out to ponder the thought of privacy. They were no longer sure if a third birthday celebration would intercept their Internet communications. As a result Phillip Zimmermann created an encryption software called Pretty Good Privacy (PGP). PGP was used to cover touchy records, but criminals extensively utilized this system to cover evidence of crimes that they had dedicated to the police.⁷

⁵ Tarun, "cyber crime ", LSI Files. P.1. accessed on <http://www.legalserviceindia.com/articles/articles/cyber.htm>

⁶ Wall. DavidS (2001). Crime and the Internet. New York, NY: Routledge.

⁷ Wall. DavidS (2001). Crime and the Internet. New York, NY: Routledge.

Interpol changed into the primary international organisation dealing with pc crime and penal rules. In conjunction with an Interpol Conference in 1981, a survey of Interpol member international locations on laptop crime and penal legislation identified several problems within the software of present penal legislation.

The Council of Europe appointed in 1985 every other professional committees so as to discuss the felony issues of computer-related crime. A precis of the suggestions for country wide legislatures with legal responsibility for worldwide acts handiest, changed into offered within the Recommendation of 1989.

These conferences caused 29 national reports, and guidelines for the improvement of pc crime legislation. Most nations in Europe followed new penal legal guidelines in step with the advice inside the Eighties and 90s. Similar improvement passed off in the U.S.A. Canada and Mexico. Also in Asia, wherein Japan, Singapore, Korea and Malaysia had been the leading countries. In Australia, the Commonwealth introduced pc crime legal guidelines to the Crimes Act in 1989.

2.3 Nature of Cyber Crime

Cyber criminal can damage web sites and portals by way of hacking and planting viruses, perform on-line frauds by way of moving finances from one nook of the globe to some other, benefit access to exceptionally confidential and sensitive facts, motive harassment by using e-mail threats or obscene fabric, play tax frauds, bask in cyber pornography involving children and commit innumerable other crimes on the Internet.

It is said that none is cozy within the cyber global. The safety is handiest for the existing moment while we're virtually relaxed. With the growing use of the Internet, cyber crime could have an effect on us all both immediately or indirectly.⁸

2.4 Classification of Cyber Crime

Cyber Crimes may be mainly categorized as: Traditional crimes devoted on or thru the brand new medium of the Internet. For instance, cheating, fraud, misrepresentation, defamation,

⁸ *Ibid*, p.141.

pornography thefts and so on. Dedicated on or through or with the help of the internet might fall underneath this class.

New crimes created with the Internet itself, together with hacking and spreading viruses and so on. New crimes used for fee of vintage crimes. For example, where hacking is committed to perform cyber frauds.

The challenge of cyber crime may be widely classified below the subsequent 3 agencies. They are:

1. Against Individuals
2. Against Organizations
3. Against Society at huge

The following are the crimes, which may be devoted in opposition to the followings organizations;

Against Individuals: –

- i. Harassment through e-mails.
- ii. Cyber-stalking.
- iii. Defamation.
- iv. Unauthorized control/access over computer gadget.
- v. Indecent exposure
- vi. Email spoofing
- vii. Cheating

Against Individual Property: -

- i. Computer vandalism.
- ii. Transmitting virus.

- iii. Netrespass
- iv. Unauthorized control/get admission to over laptop device.
- V. Intellectual Property crimes

Against Organization: -

- i. Unauthorized manage/get admission to over laptop machine
- ii. Possession of unauthorized statistics.
- Iii. Cyber terrorism in opposition to the authorities company.
- Iv. Distribution of pirated software program and so on.

Against Society at huge: -

- i. Pornography (basically infant pornography).
- Ii. Polluting the kids through indecent exposure.
- Iii. Trafficking
- iv. Financial crimes
- v. Sale of illegal articles
- vi. Online playing
- ii. Forgery

The above mentioned offences may be discussed in brief as follows:

I. Badgering by means of messages

Badgering through messages is definitely not another idea. It is fundamentally the same as irritating through letters. As of late I had gotten a mail from a woman wherein she whined about the equivalent. Her previous beau was sending her sends always once in a while sincerely

extorting her and furthermore compromising her. This is an exceptionally basic sort of provocation through messages.

II. Digital stalking

The Oxford word reference characterizes stalking as "seeking after stealthily". Digital stalking includes following a man's developments over the Internet by posting messages (now and then compromising) on the announcement sheets frequented by the person in question, going into the talk rooms frequented by the person in question, always besieging the injured individual with messages and so forth.

iii. Unauthorized control/access over computer system

This movement is normally alluded to as hacking. The Indian law has anyway given an alternate implication to the term hacking, so we won't utilize the expression "unapproved get to" conversely with the expression "hacking" to avert disarray as the term utilized in the Act of 2000 is a lot more extensive than hacking.

IV. E- mail spoofing

A spoofed e-mail can be said to be one, which misrepresents its beginning. It suggests it's beginning to be exclusive from which actually it originates.

Recently spoofed mails have been despatched at the name of Mr. Navix Ayesha kar (naavi.Org), which contained virus.

V. Dissemination of obscene material

Pornography on the internet may additionally take diverse paperwork. It may additionally consist of the hosting of net website containing these prohibited substances. Use of computers for generating those obscene substances. Downloading via the Internet and obscene materials.

vi. Intellectual Property crimes

Intellectual property includes a package of rights. Any illegal act with the aid of which the owner is disadvantaged absolutely or in part of his rights is an offence. The commonplace form of IPR

violation may be stated to be software piracy, copyright infringement, trademark and provider mark violation, theft of laptop source code, etc

vii. Trafficking

Trafficking may also expect one of a kind paperwork. It may be trafficking in tablets, humans, palms weapons etc. Such kinds of trafficking are going unchecked due to the fact they may be carried on below pseudonyms. A racket turned into busted in Chennai where capsules have been being offered underneath the pseudonym of honey.

2.5 Characteristics of Cyber Crime

After the grouping of digital wrongdoing and before analyzing the lawful methodologies to check digital wrongdoing, it is important to look at the impossible to miss attributes of digital wrongdoing.

The weapon with which digital wrongdoing are submitted is innovation. Digital violations are crafted by innovation and in this way digital lawbreakers are technocrats who have profound comprehension of the Internet and PCs.

Digital wrongdoing knows no land confinements, limits or separations. A digital criminal in the one corner of the world can carry out hacking on a framework in the other corner of the world for instance a programmer in the US can progressively hack in the framework put in Japan.

Every one of the parts of digital guiltiness from planning to execution, occur in the internet.

Digital wrongdoing has the capability of causing damage and damage which is of an impossible greatness. It can undoubtedly crush sites made and kept up with colossal speculations or hack into site of Banks and the guard division's sites.

It is to a great degree hard to gather proof of digital wrongdoing and demonstrate the equivalent in the Court of law, because of the namelessness and imperceptibility of digital criminal and its

capability to influence in a few nations in the meantime, which are not quite the same as the place of activity of the digital criminal.⁹

⁹ *Ibid*, pp.141-42.

Chapter III

Legal Approach cyber crime prevention in Bangladesh

3.1 National legislation Protecting Cyber crime

In this chapter I am going to discuss about the how to protect the Cyber Crime in Bangladesh and how to apply the National Legislation and International Legislation to Prevent Cyber Crime.

3.1.1 Information and Communication Technology Act, 2006

Cybercrime is the new and chief most concerning issue in our nation. In any case, we have no any adequate law behind this. Be that as it may, we have an Act for controlling the cybercrime named Information and Communication Technology Act, 2006. In these Act areas 56, 57,66,67,68 portray the way and the exercises of the cybercrime.

In segment 56 obviously if any individual with purpose and furthermore monitoring the impact from doing such things like harm or changed any think which is connected with the PC likewise treated as wrongdoing under this Act.

It is illicit and this is the hacking offense based on this Act. He likewise rebuffed somewhere around seven years and which will be raised up to fourteen years additionally and furthermore condemned with fine. Section 57 additionally said about the cybercrime as like-if any obstinately distribute any off scene video or picture in the web which may destructive for the general public and furthermore that individual and on the off chance that it is fall false, it will turn as an offense under the Act. He additionally rebuffed detainment for term not surpassing fourteen years and at least seven years and furthermore rebuffed with fine, which isn't surpassing one million taka.

The court additionally pursues the section 3 of Code of Criminal Procedure. At the point when any wrongdoer is missing at that point court advises him by distributing in paper. Here likewise clarified that the safeguard strategy, however it isn't clear completely in the digital related issues; I suspect as much.¹⁰

¹⁰Section 3 of Criminal Code of Procedure 1865

According to the ICT Act the cybercrime shall be treated as non-cognizable offence that is why the police can't arrest the criminals without warrant except some cases. That is why the police can't arrest the criminals without warrant except some cases. But we can see here that no any other specific Act for combating cybercrime. Here also a short description is mentioned, not a full form of cybercrime. On the basis of ICT Act I realize that in this Act enacted for all classes of electronics related crime not only cybercrime.

3.1.2 Digital Security Act 2016

The ICT Department of the Ministry of Telecommunications has concluded the draft of the Digital Security Act, 2016 and it's been put for bureau endorsement. This Act is coming as an updated version of the digital assurance law of the state, and could supplant a part of the disputable arrangements of virtual safety legal guidelines, similar to region 57 of the ICT Act 2006.

Some essential highlights of the draft Digital Security Act, 2016 - It perceives and characterizes E-Commerce, E-Transactions. In vicinity four of the draft Act represents the locale of the Act, which covers the two people interior and beyond the outskirts of Bangladesh.

Area five says about constitution of a Digital Security Agency, who will screen and oversee the advanced substance, interchanges mediums such as cellular phones to expect digital wrongdoing. This area additionally affords Digital Forensic Lab and Bangladesh Cyber Emergency Incident Response Team (Bangladesh-CERT).¹¹

In plainly I clarify that the section 2 of Digital Security Act 2016 characterizes that what is legitimate access, unlawful access, basic data framework, e-exchange, e-installment, information debasement, information, program, computerized organize, endorser data, activity information, electronic phony, advanced sex entertainment, advanced tyke sex entertainment and so on. Yet, in other area depict to capacity and chronicling the archives. Be that as it may, how stockpiling it isn't referenced in this Act.

¹¹Section 7 of Digital Security Act 2016 (draft)

3.1.3 Pornography Act 2012 and Child Pornography

To ensure the ladies and tyke and grown-up from sexual video, inappropriate behavior and furthermore coercing and to anticipate boundless of video, MMS, picture through portable or any way however referenced the web. In eighth March, 2012 this Act is authorized. In segment 2 depict the meaning of erotic entertainment.¹² In section 5 depict the examination methodology and alternate areas additionally portray the system of discipline and other such issues. In any case, there has no any words which are plainly related with the digital ¹³

Be that as it may, there has no other explicit Acts and not have some other exceptional rule to forestall tyke cybercrime or really youngster sex entertainment by any means. In short I comprehend that - Anti-erotic entertainment act(2012) has been authorized by the legislature of Bangladesh to make a confinement in the sharing and making sex entertainment by the people as it brings a crushed outcome for the individual associated with it as well as for the more noteworthy society.

Section 4 expressed that-Pornography generation, stockpiling, advertising, convey, supply, buy, move, hold or can't be shown.¹⁴

Section 7 Investigation of any offense submitted under this Act or the specialized master confirmed by the able expert over the span of the offense has been focused on the legislature, independent, semi-self-sufficient association accountable for the specialized bureau of a permit or approval from the Government and private people or any individual or association Technical able foundations responsible for the licensed people will be treated as the sentiments of specialists from the remarks got and it might be utilized as proof in court.¹⁵

Section 10- Offense committed under this Act shall cognizable and non-billable.¹⁶

¹²Section 2 of Pornography Act 2012

¹³Section 5 of Pornography Act 2012

Section 11-Offense carried out under this Act will be as per the strategy depicted in the Code of Criminal Procedure. Given that the Government, by warning in the official Gazette, an exceptional court or council to pass judgment on violations submitted under this Act may assign powers.

3.1.4 Penal Code 1860

Penal code 1860 describe the cybercrime contain crook sports which might be conventional in nature, which include theft, fraud, forgery, defamation and mischief, all of which can be problem of penal legal guidelines of our Court. The abuse of computer systems and additionally internet or cyber also given start to a gamut of new age of crimes which are addressed with the aid of the special laws enacted to penalize these crimes. For instance ICT Act 2006 defines certain offence which does no longer cover with the aid of the Penal Code.

But in case of cybercrime like Hacking, Internet time thefts, Email bombing- there may be not anything contained in our penal code. So it may be said that it isn't possible for our authorities to control cybercrime by way of the use of a few provisions of the penal code .To managed cybercrime it is necessary to enact special regulation which only offers with cyber associated subjects

3.1.5 Bangladesh Telecommunication Act 2001

The Bangladesh Telecommunication Act 2001 has created a powerful regulatory authority within the telecommunication region and segment 53 of the Act gives the arena enough electricity to intercept the verbal exchange system to stop any type of undesirable cyber incidents with the use of telecommunication tools within the United States of America.

But this is additionally comparable just like the ICT Act, due to the fact there has also no extra information about the cybercrime. It is the intricate description approximately all varieties of telecommunications like mobile, internet, telephone, fax and so forth.

Chapter IV

International legislation protecting cyber crime

There are various initiatives taken by the Organizations worldwide from time to time to control the growing of cyber crime. Some of the initiatives taken by various organizations are:

4.1 The United Nation

A Resolution on preventing the criminal misuse of information technology become followed via the General Assembly on December four, 2000 which includes as followings:

- (a) States must make sure that their laws and practice remove safe havens for the those who criminally misuse records technology.
- (b) Legal structures should defend the confidentiality integrity and availability of records and laptop structures from unauthorized impairment and ensure the criminal abuse is penalized.

4.2 The Council of Europe

Convention on Cyber Crime of 2001 is a historic milestone within the combat towards cyber crime. Member States must entire the ratification, and other States have to bear in mind the opportunity of acceding to the Convention or compare the advisability of imposing the principles of the Convention. With the Council of Europe Convention on Cyber Crime and the guidelines from, G8, OAS, and APEC, we may also attain our purpose of a international legal framework against cyber crime.

As of February 2007, the total numbers of signatures now not followed by ratifications are 22 international locations. The overall variety of ratifications/accessions at gift is 21.¹⁷

¹⁷ *Ibid*, pp.169-70.

4.3 The European Union

In the European Union, the Commission of the European Communities presented on April 19, 2002 a suggestion for a Council Framework Decision on attacks against data structures. The notion became adopted by means of the Council in 2005 and consists of Article 2: Illegal access to Information System, Article three: Illegal System Interference and Article 4: Illegal Data Interference.

Article 2 Deals with each Member State shall take the necessary measures to make sure that the intentional access without proper to the complete or any part of an records system is punishable as a criminal offence, at the least for instances which aren't minor.

Article 3 deals with the important measures to make sure that the intentional critical hindering or interruption of the functioning of an records device by way of inputting, transmitting, detrimental, deleting, deteriorating, altering, suppressing or rendering inaccessible computer records.

4.4 ASEAN

The Association of Southeast Asian Nations (ASEAN) has established high level Ministerial Meeting on Transnational Crime (AMMTC). At the Meeting in Bangkok, January 8, 2004, a statement included cyber crime was recognized and the need for an effective legal cooperation to enhance the fight against transnational crime.

Formulate Cooperative and emergency response procedures for purposes of maintaining and enhancing cyber security and preventing and combating cyber crime. In a statement from ASEAN Regional Forum (ARF) on July 2006 it was emphasized that: "Believing that an effective fight against cyber tacks and terrorist misuse of cyberspace requires increased rapid and well functioning legal and other forms of cooperation."¹⁸

¹⁸*Ibid*, p.171.

4.5 APEC

The Ministers and leaders of the Asia Pacific Economic Cooperation (APEC) have at a assembly in 2002 made a dedication to: “Endeavor to enact a comprehensive set of laws relation to cyber protection and cyber crime which are constant with the supply of worldwide prison gadgets, such as United Nations General Assembly Resolution fifty five/63 (2000) and Convention on Cyber crime (2001) by way of October 2003.”

In a Ministerial Meeting in Santiago, Chile, November 2004, it was agreed to bolster the respective economies ability to fight cyber crime with the aid of enacting domestic rules constant with the provisions of international prison gadgets together with the Convention on Cyber Crime (2001) and relevant United General Assembly Resolutions.¹⁹

4.6 Organization of American States

The Ministers of Justice or Ministers or Attorneys General of the Americas inside the Organization of American States (OAS) endorsed in Peru in 1999 the establishment of a group of government specialists on cyber crime. At a assembly in Trinidad and Tobago in 2002 suggestions have been adopted giving the Group of specialists the following mandate:

“To bear in mind the Preparation of pertinent inter-American criminal devices and version regulation for the cause of strengthening hemispheric cooperation in preventing cyber crime. Considering requirements referring to privateness, the protection of statistics procedural factors and crime prevention.²⁰”

4.7 International Criminal Police Organization (Interpol)

Many international companies qualify for professional organizations, due to the fact their dreams and sports are focused on sure specific issues; these groups consist of Interpol, the International Telecommunications Union, and so on. However, professional efforts right here broadly speaking imply giant actions inside the area of cyber protection safety and cybercrime

¹⁹*Ibid*, p.171-72.

²⁰ *Ibid*, p.173.

prevention. Although some different corporations also substantially make contributions to coordinating cyber safety safety, their emphasis is not always at the law. By this fashionable, this section best analyzes the actions of the International Criminal Police Organization (Interpol)

4.8The Organization for Economic Cooperation and Development (OECD)

With its 30 part nations, the OECD tended to PC security for quite a few years. In 1983, a specialist board of trustees was delegated by the OECD to talk about PC wrongdoing wonders and criminal-law change. Offenses against privacy, uprightness or accessibility recorded in the 1985 OECD archive included unapproved get to, harm to PC information or PC programs, PC attack, unapproved capture attempt, and PC secret activities.

4.9Treaties & International Agreements on Cyber Crime

4.9.1 United Nations Convention against Transnational Organized Crime (2000)

This arrangement, otherwise called the Palermo Convention, commits state gatherings to sanction residential criminal offenses that objective composed criminal gatherings and to receive new systems for removal, shared lawful help, and law implementation participation. In spite of the fact that the bargain does not unequivocally address digital wrongdoing, its arrangements are exceptionally important.

4.9 .2 Convention on the Rights of the Child (1989)

Article 34 of the Convention commits state gatherings to shield kids from all types of sexual misuse and misuse, including prostitution and sex entertainment.

4.9.3 Optional Protocol to the Convention on the Rights of the Child (2001)

This convention to the 1981 Convention tends to the offer of kids, youngster prostitution, and kid erotic entertainment. Article 3(1)(c) restricts the creation, appropriation, scattering, deal, and ownership of kid erotic entertainment. The Preamble makes reference to the Internet as a methods for circulation. The meaning of tyke sex entertainment, put forward in Article 2(3), is sufficiently wide to include virtual pictures of youngsters.

4.10 Digital Security Act Legal Provision

The ICT Department of the Ministry of Telecommunications has finished the draft of the Digital Security Act, 2016 and its been set for bureau endorsement. This Act is coming as an updated form of the digital insurance regulation of the country, and could supplant a portion of the disputable preparations of digital safety laws, much like region fifty seven of the ICT Act 2006.

Section 5 says approximately charter of a Digital Security Agency, who will display and modify the superior substance, interchanges mediums such as cell telephones to forestall virtual wrongdoing. This segment moreover presents Digital Forensic Lab and Bangladesh Cyber Emergency Incident Response Team (Bangladesh-CERT).

Section thirteen of the Act indicates the Power of the DG of Digital Security Agency, where the DG can set up a restrict on correspondence in extra common condition (protection rupture or country wide-accepted threat) to any person or specialist employer.

Section 15 of the Act delineates the virtual wrongdoings in sort of Hacking, pantomime, infringement of protection and one of a kind methods.

Section sixteen delineates the Punishment for the offenses under region 15 (virtual wrongdoings, functional publicity against Liberation War or Bangabandhu), walking from three years Prison sentence to Life Imprisonment as well as a quality of 10 Million taka.

Section 21 envelops the comparative offense of any man or woman who helps or abets the fee of any offense below the Act, and will be qualified for comparative discipline.

The initial under the Digital Security Act will be held on the equal Cyber Tribunal that changed into constructed up under the ICT Act 2006; the systems of the Tribunal could be comparative too – ultimate the preliminary inside one hundred eighty days.

Chapter V

Challenges for Implementation or Combating Cyber Crime

5.1 National Plan

It is extremely hard to make another law. Due to, in the event that we need to influence another law we need to keep running all the while, which is hard method for us. First and for most essential thing is that we need to make a national arrangement to battle that sorts of wrongdoing. The legislature should make an arrangement where all cooperates to address the danger of cybercrime. Hence, I think which laws we have are not adequate, really this Acts are not made for just digital related issues. To involve this looked for of laws we need to pursue a few tenets like:

5.1.2 Understanding the issue

Right off the bat, we need to understand the issue, really the advanced issue. Presently multi day all are completely associated with the web and consequently they are getting wrongdoing by the web and they are same as would be expected crooks. So we need to discover the kinds of offenses and after that we can get a choice. In any case, in our laws I can't discover any segments which characterize how to comprehend the issue.

5.1.3 Partnerships and shared duty; singular wrongdoing

Cybercrime is an individual kind wrongdoing however now and then it will be made by a gathering, yet this is extremely uncommon. While, independently we can't battle it, to embroil it we need to work by a gathering or organization work and get an individual duty. At that point we can diminish it. In our Acts obviously how to examine and who has the ability to explore. Be that as it may, there has not make reference to the framework how they function in this field.²¹

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

5.1.4 Focusing on avoidance

Our laws have no any segments which can expand the arrangement of concentrating on aversion. In any case, we need to inspire focus to keep that wrongdoing for eternity. On the off chance that we bound by the law to settled the objective for anticipate it then this wrongdoing will be halted.

5.1.5 Balancing security opportunity and protection

The web is based upon the opportunity, imagination and development of clients. In endeavoring to make a progressively secure online condition and make a move against digital culprits, our reaction must adjust the privileges of digital clients and furthermore our nation arrangement. We should mind of people's entitlement to protection. However, it is sorry to learn that these sorts of activity approach are not planned in our Acts.

5.2 Law Makers on the Basis of Cyber

In our advanced period or digitalization nation needs to make another body that is absolutely extremely wise on the field of digital or web. In our nation we have no such individual body to make laws based on web. Characteristic knowledge is making laws. They aren't notable about the web obviously. Now that is the issue, that when they have very little thought regarding it then how they establish laws on this? Since they just observe the issues however they won't realize how to take care of these issues. Furthermore, they make laws which are not appropriate for that circumstance. So I think whether we make bodies which are comprised with IT authority, at that point we can get a proper Act on this area.

5.3 Law Ministry on the Basis of Cyber

We have no any individual service based on digital related issues or based on web division. Be that as it may, now daily it is a major issue in our general public. Numerous individuals are submitting such offenses quickly as like the characteristic guilty party.

In light of we have no any watchman on this. On the off chance that our administration makes a service, we will be protected from the digital culprits. Since this service is our watchman. What's more, I think whether we have a gatekeeper then we can make laws on our interest and this service comprises with the researchers.

5.4 Public Awareness about Cybercrime

It is critical to advise to the general population pretty much a wide range of issue about digital wrongdoing. In the event that they are not notable about that issue unmistakably, they may submit such offense. On the off chance that we through our eyes to that issue we can see that, the present we have no any mindfulness about the digital wrongdoing. Hence, we are submitting such kinds of offense.

5.5 Internet Based Education

The present kids are tomorrow's future. Be that as it may, in our instructive framework depends on books. We need to illuminate them about the digital related issues by their exercises. Else they will be submitted digital offense for their absence of education on this part. Bangladesh government ought to do this. Be that as it may, where are they? Simply making laws are not the duty but rather likewise execution is the correct method to secure the general public. So web based training is the imperative thing to stay away from cybercrime.

5.6 Digital Security

Our nation has no any solid security, consequently our framework is hacked by numerous culprits in a few times. On the off chance that our security is hard, it won't be done any longer. We have additionally a Digital Security Act 2016. Be that as it may, this Act additionally as like as ICT Act 2006. This Act isn't adequate to battle cybercrime. We should make a most grounded security Act. Generally our nation will be hampered step by step.

5.7 Investigational Power and Investigational System

By our laws it is indicated that somewhere around a sub-overseer can examine it. Yet, on the off chance that he isn't clever about that looked for of issue, what will be finished? It completely pulverized due to his lack of education about digital related issue. This investigational framework is same as other wrongdoing moreover. Is the other wrongdoing and the cybercrime is same? In the event that the examination contributed to the researchers who are outstanding about the digital wrongdoing. At that point we can depend on it and we can get a superior examination report. The examination framework is as like as different cases.

Chapter VI

Comparative Case Study

6.1 Cyber crime in different international locations

Cybercrime has been within the information recently, whether or not it was the hack of the Democratic Party inside the US during the most latest presidential election, or a scam that sent fake Google Docs hyperlinks to people's Gmail debts.

6.1.1 The United States

The US got here out manner in front of each other us of a on Symantec's listing. Last 12 months it was wide variety two, with 18.89% of threats detected globally, however that has risen to 23.96%.

6.1.2 China

China turned into the second one-biggest supply of worldwide threats detected by using Symantec, down from the number one spot final 12 months. CNBC mentioned in July that malware that originated in China were found to have infected over 10 million Android phones.

6.1.3 Brazil

Brazil has the doubtful honour of entering Symantec's pinnacle 3 international locations for danger detections. It has had a huge upward push, up from quantity 10 ultimate year. Security Intelligence published an outline of the trends in Brazilian malwareback in July.

6.1.4 India

India honestly went down Symantec's leaderboard of global threat detections. This yr it is quantity 4, while last yr it was at quantity three. It turned into reported in February that Hitachi's ATM gadget in India have been compromised for 2 months.

6.1.5 Germany

Germany came in at wide variety five on Symantec's listing, up from number eight last year. The united states has been a target of malware within the past: In 2016 a German nuclear plant changed into located to be inflamed with computer viruses.

6.1.6 The United Kingdom

The UK came in 7th in Symantec's ranking, the identical role as 2015. Research from the Enigma Software Group launched in March confirmed that London and Manchester are the most probable cities in the UK for computer systems to be infected with malware.

6.2 Cyber Crime related case:

One billion user accounts stolen from Yahoo, 2013

In one in all the most important instances of statistics robbery in records, Yahoo had statistics from more than one billion user debts stolen in 2013.

Personal information along with names, cellphone numbers, passwords and e-mail addresses were taken from the net large. Yahoo claimed on the time that no bank details were taken.

Releasing statistics of the breach in 2016, it become the second one time Yahoo were targeted by using hackers, after the bills of nearly 500 million users have been accessed in 2014.²²

Sony Pictures crippled by GOP hackers, 2014

In late 2014, important entertainment agency Sony Pictures had been hit with a crippling virus.

Cyber crime organization Guardians of Peace (GOP) have been at the back of the obvious blackmail try, which noticed around 100 terabytes of sensitive facts stolen from the company.

It is largely idea that the assault turned into related to North Korea's disapproval of the movie 'The Interview', which humorously expected Kim Jong-un and contained a plot where primary characters tried to assassinate the pinnacle of state.

US government agencies investigated the claim that North Korea had authorised the cyber attack in an attempt to prevent the film from being released.²³

Chapter VII

Findings and Conclusion

7.1 Findings:

The ICT Act has identified some crucial scenario, which is not clean to our archaic criminal provisions. The regulation does something modify the social norm after which manipulate of information generation. Ever for the reason that passing of the Information and Communication Technology Act by parliament, lots has been stated both for and in opposition to the Act. Although the newly enacted Cyber Law has some weak spot, something is higher than not anything.

Cyber Offences Investigation Police Officer must have applicable information: Under phase eighty of the ICT Act, 2006 that a police officer no longer under the rank of an Inspector of Police shall investigate any offences under this Act. This section should be changed that Inspector of Police and above, should have suitable ICT information (i.E. Diploma/Bachelor's diploma in ICT related problem right training in this vicinity. The draconian strength had been given to law enforcement officials that a police officer not below the rank of an Inspector of Police (IP), or any other officer of the Government legal with the aid of the Government on this behalf for motive of investigating and stopping the fee of a cyber crime underneath phase of the ICT Act, 2006.

There is not any provision about the Intellectual Property Rights of "domain Name" proprietors. These need proper interest. Section 56 of the ICT Act, 2006, that the order of the Government appointing any person as the Presiding officer of a Cyber Appellate Tribunal will be final and shall now not be referred to as in question in any manner and no Act or proceeding before a Cyber Appellate Tribunal shall be called in question in any way at the ground merely of any defect in the charter of a Cyber Appellate Tribunal.

The Government cannot claim immunity in appointment to Cyber Appellate Tribunal, as the same is opposite to the spirit of the Constitution of Bangladesh. So, beneath the Constitution of Bangladesh, all proceeding and Act of the Cyber Appellate Tribunal are null and void-ab-initio.

Some others troubles are Difficult to discover the cyber criminals: Now a day's cyber crime has been spreading all over the global to a amazing volume.

Behind that the maximum important motive is to devote cyber crime, no physical presence is needed immediate. Generally the criminals take place this crime using the highest privileges of

the technology sitting one corner of the arena. So it is clearly difficult to perceive the cyber criminals.

7.2 Conclusion:

As we flow ahead into the twenty first century, technological innovations have paved the way for us to revel in new and brilliant conveniences inside the how we're educated, the manner we store, how had been entertained and the way wherein we do commercial enterprise. Capacity of human minds is immeasurable. It isn't always viable to remove cyber crime form the cyber area. It is pretty feasible to test them.

The simplest feasible step is to make humans aware of their rights and responsibilities and in addition making the utility of the laws greater stringent to check crime. Undoubtedly the ICT Act is a historical step inside the cyber world.

So laws ought to be evolved in any such way that crimes in the area of technological arena may be controlled in an iron hand. But no such powerful criminal provisions exist at domestic and overseas. Though there are a few laws and conference, they cannot be applied due to a few technical problems like procedural complexities and shortage of proper executing machine.

Taking those blessings, the criminals are going on heinous crimes like Hacking, Sending malicious mails, spreading vulgar pix, cyber terrorism & and illegal the usage of of highbrow homes. It causes harm to the privateness of individuals as well as creates danger to the international peace and harmony. Now it is the call for of time to prevent such type of crimes for maintaining character privacy in addition to global peace and protection. Every United States of America of the sector can enact effective legal provisions within the purview in their national boundary to guard cyber crimes. United Nations also can take vital steps to save you cyber crimes from the cyber space.

Bibliography

Books

1. Narayan, P. Intellectual Property law, (India: Eastern Law Publishing Co. Pvt. Ltd,2001)
2. Ahmed DR. Zulfiqar, A Text Book On Cyber Law in Bangladesh
3. D Rodney Ryder, Guide to Cyber Laws, 2nded. (Nagpur:Wadha & Company, 2005)
4. Abdul Halim & N. E. Siddiki, The Legal System of Bangladesh after Separation, 1st ed., (Dhaka: University Publications, 2008).
5. N. V. Paranjape,Criminology and Penology, 13th ed., (Allahabad: Central Law Publications, 2008-09).
6. R. K. Chaubey, An Introduction to Cyber Crime and Cyber Laws, 1sted., (Kolkata: Kamal Law House, 2009).
7. Zulfiqar Ahmed, A Text Book on Cyber Law in Bangladesh, 1st ed., (Dhaka: National Law Book Company, 2009).
8. Cyber Law in Bangladesh (Information and communication Technology Act,2006) Media, Press and Telecommunication Laws in Bangladesh.
9. Media and Cyber Laws in Bangladesh (Telecommunication, print, Broadcast, Film and Online Media Law with commentary and case law)

List of Statutes

1. Information and Communication Technology Act (ICT), 2006.
2. Digital Security Act 2016 (draft)
3. Penal Code 1860
4. Bangladesh Telecommunication Act 2001
5. Criminal Code of Procedure 1898
6. Pornography Act 2012
7. The Computer Misuse Act (1990).
8. The Computer Fraud and Abuse Act, 1984.
9. The United Nations Commission on International Trade Law (UNCITRAL), 1996.
10. The Bankers' Books Evidence Act, 1891.

11. The Bangladesh Bank order, 1972.
12. The Lunatic Act, 1912.
13. The Convention on Cyber Crime, 2001.

Cases

1. One billion user accounts stolen from Yahoo, 2013
2. Sony Pictures crippled by GOP hackers, 2014
3. Hackers steal £650 million from global banks, 2015

Journals

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

Websites

- 1.<http://www.naavi.org/pati/pati_cybercrimes_dec03.htm>
2. <Daily ProthomAlo (12 March, 2012),<http://www.bangladeshnews24.com/prothomalo/newspaper/>>
3. <<http://www.slideshare.net/fakrulalam/bangladesh-cyber-security-status-in-global-perspective>>
4. < <http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>>
5. <<http://www.mid-day.com/articles/cyber-crime-doubles-in-navi-mumbai-in-2-years/15989157.>>
6. <<http://tech.firstpost.com/news-analysis/5-things-all-broadband-users-must-know-81724.html>>
7. <<http://wirelessbangladesh.blogspot.com/2009/04/internet-history-of-bangladesh.html?m=1>>
8. <<httpwww.bdlawdigest.orgcyber-crime-a-new-menace-in-modern-era>>
- 9.<<http://www.risingbd.com/english/cyber-crime-in-bangladesh-a-growing-threat-in-digital-marketplace/28940>>
10. <<http://www.progressbangladesh.com/maximum-14-tears-in-jail-for-cyber-crimes/>>

