UGC & Govt. Approved

Sonargaon University (SU)

সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph

On

Cyber Crime Trial System in Bangladesh: Problems and Prospects.

A Thesis Submitted in Partial Fulfillment of the Requirments for the Degree of LL.M. Department of Law, Sonargaon University (SU)

Prepared By:

Rashedul Islam

ID No. LL.M 2103024020

Program: LL.M.

Department of Law

Sonargaon University.

Supervised By:

Sanjoy Pal

Lecturer and Coordinator

Department of Law

Sonargaon University.

Date of Submission: 05 September 2022.

Letter of Tranmittal

To
Sanjoy Pal
Lecturer and Coordinator
Department of Law
Sonargaon University

Subject: **Submission of Research Monograph on "Cyber Crime Trial System in Bangladesh: Problems and Prospects"**

Dear Sir,
This is a great pleasure to submit the Research Monograph on "Cyber Crime Trial System in Bangladesh: Problems and Prospects" as a partial requirement for the fulfillment of LL.M (1year) under the Department of Law of the Sonargaon University (SU).

I have given due efforts to this Research Monograph as faithful and informative as possible. I hope that this paper will not be the formality of academic course completion, rather it will be a good source of information for future research on this topic.

Yours Sincerely

Rashedul Islam
ID No. LL.M 2103024020
Department of Law
Sonargaon University

Declaration

I am fully aware that I have an obligation to make it clear to the assessor as to which is my own work and which is the work of others I will be citing in my paper. Unless, I clearly indicate otherwise, my assessor is entitled to assume that everything being presented in the paper originates from me.

Signature

Supervisor's Certificate

This is to certify that the work presented in this dissertation is based on the work carried out by the author herself under my supervision in the Department of Law, Sonargaon University (SU).

It is also certified that the work presented here is original and suitable for submission in terms of its style and contents for fulfillment of LL.M (1year) Program.

Sanjoy Pal
Lecturer and Coordinator
Department of Law
Sonargaon University

Acknowledgement

"In the name of Allah, the Beneficent, the Merciful"

All praise be to Almighty Allah for enabling me to finish this Research Monograph. I am very happy to complete it. It is a great research of my life. It is a long cherished hope of my life to become a great lawyer. That's why I have admitted in the Department of law in Sonargaon University (SU) to fulfill my dream. But through ought my whole academic life in this field, I did not get mach opportunities to examine and show my knowledge and skill in this wide field. Finally I hope got a great opportunity to make my study meaningful when I got the chance to prepare a Research Monograph on **"Cyber Crime Trial System in Bangladesh: Problems and Prospects".**

I express my sincere thanks to Sanjoy Pal, Lecturer, Department of Law, Sonargaon University for his guidance, advice, help throughout the entire course and specifically when acting as my supervisor for this research.

I am also thankful to my classmate as they helped or assist me to complete the Research Monograph. I am extremely thankful to all the authors and writers whose works helped me to draft this original Research Monograph.

Lastly, I thank the Almighty for being always there for me.

ABSTRACT:

Cyber and technology related crime is gradually increasing in Bangladesh. It is a significant issue in Bangladesh. It has already been seen that a glomming threat becomes visible in the arena of information technology. Recently the hacking of RAB website and e-mail threats of former prime minister is example for few of them. In contrast, 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 Digital Technology Act-2006 and ICT (Amendment) Act-2013 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 article incorporates the impacts of cybercrime in Bangladesh especially focuses on the area of Personal life, Workplace as well as Policy making Bodies or thinkers. I believe that this article would help all relevant concerns and especially policy makers.

Key Words: Cybercrime, Cyber Criminal, Impact, Criminal Profile, Legislation.

Table of Contents

Letter of Transmittal
Declaration
Supvervisor Certificate
Acknowledgement
Abstract

Chapter-I

S.L. NO.	Topic	Page No.
1.1	Introduction	01
1.2	Problems	02
1.3	Objectives	02
1.4	Cybercrime	03

Chapter-II

S.L. NO.	Topic	Page No.
2.1	Types Of Cybercrime With The Profile Of Cyber Criminals And Victims And Reasons	04
2.2	Hacking	05
2.3	Virus Dissemination	05
2.4	Software Piracy	05
2.5	Pornography	05
2.6	Credit Card Fraud	06
2.7	Sale of Illegal Articles	06
2.8	Online Gambling	06
2.9	Intellectual Property Crimes	06
2.10	Email Spoofing	07
2.11	Cyber Defamation	07
2.12	Cyber Stalking	07
2.13	Email Bombing	07
2.14	Data Diddling	08
2.15	Salami Attacks	08

Chapter-III

S.L. NO.	Topic	Page No.
3.1	Reasons Of Cybercrime	09
3.2	Capacity to store data in comparatively small space	09
3.3	Easy to access	09
3.4	Complex	09
3.5	Negligence	10
3.6	Loss of evidence	10

Chapter-IV

S.L. NO.	Topic	Page No.
4.1	Profile of cyber criminals	11-12
4.2	Impact of Cybercrime against individuals	12
4.3	Harassment via e-mails	12-13
4.4	Cyber-stalking	13
4.5	Pornography	13
4.6	Defamation	13
4.7	E-mail spoofing	14
4.8	Fraud & Cheating	14

Chapter-V
Impacts against Individuals Property

S.L. NO.	Topic	Page No.
5.1	Computer Vandalism	15
5.2	Transmitting Virus/Worms	15
5.3	Logic Bombs	16
5.4	Trojan Attacks	16
5.5	Web Jacking	16-17
5.6	Internet Time Thefts	17
5.7	Intellectual Property Crimes / Distribution of Pirated Software	17

Chapter-VI
IMPACT OF CYBERCRIME AGAINST ORGANIZATIONS:

S.L. NO.	Topic	Page No.
6.1	Unauthorized Control/Access over Computer System	18
6.2	Possession of unauthorized information	18
6.3	Software Pirate and Copyright	19
6.4	Financial Institutions are at risk	19

Chapter-VII

S.L. NO.	Topic	Page No.
7.1	Impact of Cybercrime against the Government	20
7.2	Cyber terrorism against the government organization	20-21
7.3	Legal Response to Cyber Crime in Bangladesh	21-22

Chapter-VIII

S.L. NO.	Topic	Page No.
8.1	Necessary Legislations in Bangladesh to Tackle Cybercrime	23-24
8.2	Cyber Tribunal	25-26
8.3	Cyber Appellate Tribunal	26

Chapter-IX

S.L. NO.	Topic	Page No.
9.1	Conclusion	27

Chapter-I

1.1 INTRODUCTION:

Cybercrime has had a short but highly eventful history. Apart from being an interesting study by itself, observing the history of cybercrime would also give the individual and society the opportunity to avoid the mistake made in past. The past recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage[1]. In 1994 the first online bank opened, called First Virtual. This opened up a lot of opportunities for hackers. Cybercrime was slowly becoming more popular. In 1995 the Secret Service and Drug Enforcement Agency (DEA) obtained the first Internet wiretap, which is exactly like a phone wiretap. The DEA was able to shut down a company who was selling illegal cell phone cloning equipment[2]. There is sharp rise in the Cybercrimes in Bangladesh and the Law enforcement machinery is finding it really it really difficult to manage these technical crimes in Bangladesh. Cybercrime has already become a going concern in both private as well as public sector in Bangladesh. During the last decade private and public sector has done a revolution with the use of technical enhancement. Due to unauthorized intervention to the system, company loses huge confidential information which caused a large amount of financial lose. It has already been identified that especially Financial Institutions are in the most threading organization for cybercrime that at the same time reflects to the personal life. Some development partners have started working how to tackle cybercrime and improve effective communications.

---

1) Verton, Dan (2003), Invisible threat of cyber-terrorism, New York, NY: McGraw-Hill/Osborne.
2) Ahmed, Dr. Zulfiquar, 2012 - Cyber Law in Bangladesh, National Law Book Company, Dhaka, pp-221-265

1.2 PROBLEMS:

Cybercrime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more. Although the term cybercrime is more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, this term is also sometimes used to include traditional crimes, such as fraud, theft, blackmail etc., in which computer or networks are used. As the use of computers has grown, cybercrime has become more important. Cybercrime, as a transnational crime, is a global issue with a global impact. Increased sophistication of cybercrime attacks and vulnerability of information available online is a serious concern for institutions, law enforcement agencies and other stakeholders. Victims of these attacks are not just private citizens or organizations with limited resources available to protect themselves but very large companies.

1.3 OBJECTIVES:

The overall purpose of the article was to identify the impact of cybercrime in Bangladesh with regard to technological enhancement.

The study has embarked upon the specific objectives are to assess:

a) Types of cybercrime with the profile of cyber criminals and victims;
b) Impact of cybercrime against individuals;
c) Impact of cybercrime against organizations;
d) Impact of cybercrime against the Government;
e) Necessary Legislations in Bangladesh to tackle Cybercrime.

1.4 CYBERCRIME:

In Generally Cybercrime may be said to be those offences, of which, genus is the conventional Crime, and where either the computer is an object or subject of the conduct constituting crime.

An prominent Advocate Daggal Pawan Specialist on cybercrime define as "Any criminal activity that uses a computer either an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime"[3]. Another definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both"[4].

Cybercrimes can be defined as 'Crime against individual or organization by means of computer is called cybercrime. Cybercrimes are those crimes which are committed in a network environment or on internet.

---

3) Tarun,2013"CyberCrime",LSI.p.l.accessedon,http://www.legalse rviceindia.com/articles/cyber.h tm
4) Karzon Sheikh Hafizur Rahman, 2008-Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, pp-411-418

Chapter-II

2.1 TYPES OF CYBERCRIME WITH THE PROFILE OF CYBER CRIMINALS AND VICTIMS AND REASONS:

Cybercrime is the latest and perhaps the most complicated problem in the cyber world."Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime". "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime.

There are major classes of criminal activities with computers:

1. Unauthorized use of a computer. It may be committed by stealing a username and password, or by accessing the victim's computer via the Internet through backdoor operated by a Trojan Horse program.
2. Cybercrime may be committed by creating or releasing a malicious computer program (e.g; computer virus, worm. Trojan Horse).
3. Cybercrime may be committed by harassment and stalking in cyberspace[5].

   All crimes performed by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system. The followings are the top listed types of cybercrime:

5) Nahar, Dr. Nurun, 2011- Fundamental's of cyber law, Bangladesh law book company, Dhaka, pp-15-28

2.2 Hacking

Hacking is a simple term means illegal intrusion into a computer system without the permission of the computer owner/user. Hackers usually do that with the intention of obtaining confidential information. An Active hackers group, led by one Dr. Nuker, who claim to be founder of Pakistan Hacker Club, reportedly hacked the websites of Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nation, India[6].

2.3 Virus Dissemination

Virus itself is software that attacks other software. It may cause for data loss, deduction of bandwidth speed, hardware damage etc. Trojan Horse, Time Bomb, Logic Bomb, Rabbit are the malicious software.

2.4 Software Piracy

Theft of software through the illegal coping of genuine programs or distribution of products intended to pass for the original.

2.5 Pornography

Pornography is the first consistently successful e-commerce product (Official website of the Cybercrime Investigation Cell, Crime Branch, CID, Mumbai). Deceptive marketing tactics and mouse trapping technologies pornography encourage customers to access their website. Anybody including children can log on to the internet and access website with pornographic contents with a click of a mouse[7].

---

6) Kader, Monjur, 2008- Criminology (Cybercrime),University press, Dhaka, pp-125-129
7) Boham and Haley (2002)-Internet Crime,Third Edition, McGrasw-Hill, New York, p-137

2.6 Credit Card Fraud

You simply have to type credit card number into www page of the vendor for online transaction. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner. Through falsification of computerized bank accounts cores of taka may be misappropriated. In some cases people are arrested and charged for stealing and misusing credit card numbers belonging to others[8].

2.7 Sale of Illegal Articles

Narcotics, weapons and wild life etc. are sold by posting information on websites, auction websites, and bulletin board or simply by using email communication. Many of auction sites are believed to be selling cocaine in the name of money[9].

2.8 Online Gambling

Million of websites are offering online gambling which are believed to be actual fronts of money laundering. Though it is not yet confirmed, these sites may have relationship with drug trafficking[10].

2.9 Intellectual Property Crimes

These include software piracy, copyrights, infringement, trademark violations, theft of computer source code etc.

---

8) Duggal Pawan, http://www.slideshare.net/anthony4web/cribercrimes-and-due-diligence.
9) Nagpal R- What is Cyber Crime. http://issuu.com/rohas/does/ece
10) Ronald B. Standler, Collected from Internet, See http://www. rbs2.com/crime.htm

2.10 Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. Personal Relationship may be jeopardized because of email spoofing. Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of bank's customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed email appeared to have originated from the bank itself.

2.11 Cyber Defamation

With help of computers and/ or the Internet When any defamation takes place it is called cyber defamation. It can tarnish personal image of any individual or reputation of any company, bank or institution.

2.12 Cyber Stalking

Cyber stalking involves following a person's movement across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-room frequently by the victim, constantly bombarding the victim with emails etc.

2.13 Email Bombing

Email bombing can be committed by sending huge number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of company or an email service provider) crashing. Thousands of emails are sent to the personal account or mail server until it is crashed.

2.14 Data Diddling

Data diddling may be committed by altering raw data just before it is processed by a computer and then changing it back after processing is completed. Government offices may be victims to data diddling programs inserted when private parties were computerizing their systems.

2.15 Salami Attacks

For the commission of financial crimes salami attacks are used. Here the major thing is to make alteration which is so insignificant that in a single case it would go completely unnoticed. “For example a bank employee inserts a program, into the bank servers, that deduct a small amount of money from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

Chapter-III

3.1 REASONS OF CYBERCRIME:

Hart in his work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cybercrime[11].

The reasons for the vulnerability of computers may be said to be:

3.2 Capacity to store data in comparatively small space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

3.3 Easy to access

The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3.4 Complex

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

11) http://www.asianlaws.orgiccyberlawlibrary/cc/what_cc.htm

3.5 Negligence

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

3.6 Loss of evidence

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Chapter-IV

4.1 PROFILE OF CYBER CRIMINALS:

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals

a) Children and adolescents between the age group of 6 – 18 years The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove them to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

b) Organized hackers these kinds of hackers are mostly organized together to fulfill certain objective. The reason may be to fulfill their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfill their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

c) Professional hackers / crackers their work is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are van employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

d) Discontented employees This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

4.2 IMPACT OF CYBERCRIME AGAINST INDIVIDUALS:

Cybercrimes committed against people include various crimes like transmission of child pornography and harassment through e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography constitute one of the most important cybercrimes known today. Cyber harassment is a distinct cybercrime. Harassment can be sexual, racial, religious, or other. This also brings us to another related area--violation of citizen which is a crime of grave nature.

4.3 Harassment via e-mails

Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Bangladesh police recently has taken plan to set up a special unit to curb cybercrimes. The matter has become more urgent since 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[12].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. The first two have reportedly said that they had sent the

12) Cyber Crime by parthasarathi patilhttp://www.naavi.org/pati/ pati_cybercrime_dec03.htm

mail for fun. As there is no nationwide computer infrastructure, no watchdog or security system has yet been developed in Bangladesh.

4.4 Cyber-stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

4.5 Pornography

Pornography on the net may take various forms. It may include the hosting of website containing these prohibited materials. Use of computers for producing these obscene materials and download through the Internet, obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them[13].

4.6 Defamation

It is an act of imputing any person with intent to lower the person in the estimation of the rightthinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. E.g. the mail account of Rohit was hacked and some mails were sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.

13) Daily Prothom alo_23 August, 2004

4.7 E-mail spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates. Recently spoofed mails were sent on the name of Mr. Na.Vijayashankar which contained virus. Rajesh Manyar, a graduate student at Purdue University in Indiana, was arrested for threatening to detonate a nuclear device in the college campus. The alleged e- mail was sent from the account of another student to the vice president for student services. However the mail was traced to be sent from the account of Rajesh Manyar[14].

4.8 Fraud & Cheating

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. Recently the Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer working in a call centre, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony website. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating under IPC, but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs 20,000, and was released on a year's probation.

---

14) Bal Bharati case_india, 2007

Chapter-V

Impacts against Individuals Property:

5.1 Computer Vandalism

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

5.2 Transmitting Virus/Worms

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988.

5.3 Logic Bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

5.4 Trojan Attacks

This term has its origin in the word 'Trojan Horse'. In software field this means an unauthorized program, which passively gains control over another's system by representing itself as an authorized program. The most common form of installing a Trojan is through e-mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

5.5 Web Jacking

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking

is that of the ‘gold fish’ case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded as ransom. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

5.6 Internet Time Thefts

Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa’s casethe Internet hours were used up by any other person. This was perhaps one of the first reported cases related to cyber crime in India. However this case made the police infamous as to their lack of understanding of the nature of cybercrime.

5.7 Intellectual Property Crimes / Distribution of Pirated Software

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.

The Hyderabad Court has in a land mark judgment has convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software.

Chapter-VI

IMPACT OF CYBERCRIME AGAINST ORGANIZATIONS:

6.1 Unauthorized Control/Access over Computer System

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

6.2 Possession of unauthorized information

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 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.

6.3 Software Pirate and Copyright

Results of an anonymous experiment conducted on more than 4,800 students in San Diego were presented at the American Psychological Association conference. It says that 38 percent of teenagers were involved in software piracy. In the context of Bangladesh most of the computer users are in the habit of using pirated software.

6.4 Financial Institutions are at risk

Bangladesh's financial institutions are at risk from hackers. In the country financial institutions have introduced various online features like online banking, stock exchange transactions but are not able to provide the highest security. Source said the cyber criminal networks through Internet have attacked our country's technology infrastructure.

Recently, hackers interrupted the DSE transaction, which cost the small entrepreneurs dearly[15].

15) See .www://naavi.org)

Chapter-VII

7.1 IMPACT OF CYBERCRIME AGAINST THE GOVERNMENT:

Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. In a report of it was said that internet was becoming a boon for the terrorist organizations[16].

7.2 Cyber terrorism against the government organization

At this juncture a necessity may be felt that is the need to distinguish between cyber terrorism and cybercrime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of – Osama Bin Laden, the LTTE, attack on America's army deployment system during Iraq war. Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".

16) Edaily star_news_30.10.2008

Another definition may be attempted to cover within its ambit every act of cyber terrorism. A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to –

(i) putting the public or any section of the public in fear; or

(ii) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

(iii) coercing or overawing the government established by law; or

(iv) endangering the sovereignty and integrity of the nation and a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism[17].

7.3 LEGAL RESPONSE TO CYBER CRIME IN BANGLADESH:

In order to facilitate e-commerce and encourage the growth of information technology, the ICT Act, 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or with both. However, recently our Parliament amended the ICT Act 2006, raising penalties for cyber crimes setting a minimum of 7 years imprisonment and a maximum of 14 years or a fine of Tk. 1 core or both. The bill made offences under sections 54, 56, 57 and 61 of the ICT Act, 2006 cognizable and non-bail able, empowering law enforcers to arrest anyone accused of violating the law without a warrant, by invoking section 54 of the Code of Criminal Procedure. All such offences were non-cognizable in the ICT Act, 2006. However, all

17) See, www-crime-research.org/library/cyber-terrorism.htm

concerned apprehend of the misuse of the power by the police. The ICT Act, 2006 as amended in 2013 is obviously a brilliant achievement of Bangladesh in the field of cyber law. Critics point out that still there remain certain specific limitations of the said Act as under.

(i) The Act remains silent about various intellectual property rights like copy right, trade mark and patent right of e-information and data.

(ii) The enactment has a major effect on e-commerce and m-commerce in Bangladesh. But it keeps itself mum as to electronic payment of any transaction.

(iii) The legislation was initially supposed to be applied to crimes committed all over the world; but nobody knows how this can be achieved in practice.

(iv) Spamming has become a peril in the west as such they have made anti spamming provisions in cyber law. However, there is no anti spamming provision in our Act.

(v) Domain name is the major issue which relates to the internet world thoroughly. But the ICT Act, 2006 does not define ‘domain name’ and the rights and liabilities relating to this.

(vi) The Act does not address any crime committed through using mobile phones.

(vii) This law made e-mails as evidence, conflicting with the country’s Evidence Act that does not recognize as e-mails as evidence. We hope our government would take proper initiative to get rid of the problems for ensuring a cyber crime free peaceful society.

Chapter-VIII

8.1 NECESSARY LEGISLATIONS IN BANGLADESH TO TACKLE CYBERCRIME:

Inventions, discoveries and new technologies widen scientific horizons but also bring new challenges for the legal world. Information Technology is brought by computers, computer networks, internet and cyberspace. It also brought many new problems in jurisprudence. There was insufficiency of legislation while dealing with the information technology. Throughout the world the judiciary dealing with the new problem like cybercrime, adjudication and investigation of cybercrime, intellectual property Rights issues in cyber world etc. The United Nations Commission on Internet Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996.Model Law provides that all Nation should give consideration to it, when they enact and revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Hence the most important enactment of the Bangladesh Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 has been done (Sec. 4 of the information & communication Act, 2006). Cyber crime 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 parliament of Bangladesh has enacted Information and Communication Technology Act, 2006 which defines certain activities as crime. The activities which made punishable under the Information and Technology Act of 2006 shall be the cybercrimes for the territory of Bangladesh. The activities are

i. Mischief of computer and computer system
ii. Alteration of source code of commuter
iii. Hacking in computer system
iv. Publication of false, indecent and defamatory statement or information in electronic form
v. Access in reserve system
vi. False representation and concealment of information
vii. False electronic signature certificate
viii. Transmission of secrecy
ix. Disclosing electronic signature for cheating
x. Committing crime through computers.

8.2 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.

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 circular an order in two Bangla newspapers to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall have the same power, a Sessions Court empowered to apply in its original jurisdiction. Public prosecutor shall conduct the case on behalf of the Government. Tribunal shall conclude the trial within six months from the

date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

8.3 CYBER APPELLATE TRIBUNAL:

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

Chapter-IX

9.1. CONCLUSION:

Basically, no notable cyber crime has yet been committed in Bangladesh. The gradual dependence and extensive use of computer and information technology by the financial institutions like bank, insurance company, and other non-government organizations increase the fear of commission of cyber crime here. Computer has been used as a tool of crime like making forged certificates and documents for a number of years in Bangladesh though the incident of targeting computer or computer system is very unusual.

Bibliography:

1) Verton, Dan (2003), Invisible threat of cyber-terrorism, New York, NY: McGraw-Hill/Osborne.
2) Ahmed, Dr. Zulfiquar, 2012 - Cyber Law in Bangladesh, National Law Book Company, Dhaka, pp-221-265
3) Karzon Sheikh Hafizur Rahman, 2008-Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, pp-411-418
4) Nahar, Dr. Nurun, 2011- Fundamental's of cyber law, Bangladesh law book company, Dhaka, pp-15-28
5) Kader, Monjur, 2008- Criminology (Cybercrime),University press, Dhaka, pp-125-129
6) Boham and Haley (2002)-Internet Crime,Third Edition, McGrasw-Hill, New York, p-137
7) Bal Bharati case_india, 2007

Web Pages:

1) Tarun,2013"CyberCrime",LSI.p.l.accessedon,http://www.legalse rviceindia.com/articles/cyber.h tm
2) Duggal Pawan, http://www.slideshare.net/anthony4web/cribercrimes-and-due-diligence.
3) Nagpal R- What is Cyber Crime. http://issuu.com/rohas/does/ece
4) Ronald B. Standler, Collected from Internet, See http://www. rbs2.com/ crime.htm
5) http://www.asianlaws.orgiccyberlawlibrary/cc/what_cc.htm
6) Cyber Crime by parthasarathi patilhttp://www.naavi.org/pati/pati_ cybercrime_dec03.htm
7) See .www://naavi.org)
8) See, www-crime-research.org/library/cyber-terrorism.htm

Journals:

1) Daily Prothom alo_23 August, 2004
2) Edaily star_news_30.10.2008