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

# Research Monograph

## On

# "Exploring Cyber Crime in Bangladesh: Realities and Challenges"

**This Research Submitted for the Partial Fulfillment of the award of the degree in LL.B (Hon's) Department of Law, Sonargaon University (SU), Dhaka.**


**Prepared For:**
**Department of Law**
**Sonargaon University (SU), Dhaka**

**Supervised By:**
**Sharmin Jahan Runa**
**Assistant Professor**
**Department of Law**
**Sonargaon University (SU), Dhaka**

**Submitted By:**
**Abdul Gani Shikder**
**ID: LL.B 1902017015**
**Program: LL.B (Hon's)**
**Batch: 17th**
**Department of Law,**
**Sonargaon University (SU), Dhaka.**


**Date of Submission: 6th July, 2023**

# LETTER OF TRANSMITTAL

**To**
**Sharmin Jahan Runa**
Assistant Professor
Department of Law
Sonargaon University (SU), Dhaka.

Subject: Submission of research paper on **"Exploring Cyber Crime in Bangladesh: Realities and Challenges"**

Dear Madam,

It is a great pleasure for me to submit the thesis on **"Exploring Cyber Crime in Bangladesh: Realities and Challenges"** While I doing this thesis, I have tried my level best to make this project paper to the latest standard. I think that thesis paper will fulfill your requirement and pleased you. I, therefore, hope that you would be kind enough to go through this thesis paper for evaluation.

I am always be ready for clearance of any part of my thesis.

Thanking you

**Abdul Gani Shikder**
ID: LL.B 1902017015
Program: LL.B (Hon's)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

# CERTIFICATION

This is to certify that the thesis on "**Exploring Cyber Crime in Bangladesh: Realities and Challenges**" is done by Abdul Gani Shikder in partial fulfillment of the requirements for the degree of LL.B. (Honours) from Sonargaon University, Dhaka. The thesis has been carried out under my guidance and is a record of the bonafide work carried out successfully.

……

**Sharmin Jahan Runa**
Assistant Professor
Department of Law
Sonargaon University (SU), Dhaka

# DECLARATION

I do hereby that this Research Monograph on the **Exploring Cyber Crime in Bangladesh: Realities and Challenges** have been done by me and this Research is free from all plagiarism and without help of other. I further declare that this monograph is prepared with my own effort and it was not and never submit to any institute for any academic reason.

**Abdul Gani Shikder**
ID: LL.B 1902017015
Program: LL.B (Hon's)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

# ACKNOWLEDGEMENT

At first, I would like to thank Almighty Allah for his kindness on me in accomplishing the report. I would like to express my deep sense of gratitude to my honorable and distinguished supervisor Sharmin Jahan Runa, Assistant Professor, Department of Law, Sonargaon University (SU), Dhaka for her individual suggestions, valuable time, important information and guidance during the study period that has greatly inspired me in preparing this report successfully.

It could not possible to think all those people who have contributed for the preparation of this report of course there are some very special names that cannot be forgotten. I am also grateful to the Department of Law, Sonargaon University (SU), Dhaka for providing me such an opportunity to come closer to real situation. Finally, I want to express my deep gratitude to my family members and all well wishers whose enormous helps assisted me to complete this report.

**Abdul Gani Shikder**
ID: LL.B 1902017015
Program: LL.B (Hon's)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

# ABSTRACT

Cyber and technology related crime is on the increase and current trends indicate that it will be a significant issue in Bangladesh. It has already been seen that a glomming threat becomes visible in the arena of information technology. 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 Communication Technology Act.2006, there are several clauses against cybercrime. But this Information and Communication Technology act is not the concert one. By enacting this act, there is a chance to become safe side after committing crimes. Beside the Government the Law Enforcement like the Police, RAB or other law enforcement agencies should take it as a challenge to prevent Cyber crimes.

**TABLE OF CONTENTS**

Chapter 1

## INTRODUCTION


1.1 Introduction 01
1.2 Background 02
1.3 Problems 02
1.4 Objectives and Scope of studies 03
1.5 Methodology used 03
1.6 Hypothesis 03
1.7 Duration of the studies 03
1.8 Chapterization 03
1.9 Conclusion 04


Chapter 2

## TYPES OF CYBERCRIME WITH THE PROFILE OF CYBERCRIMINALS, VICTIMS AND REASONS


2.1 Types of Cybercrime 05
2.1.1 Hacking 05
2.1.2 Virus Dissemination 05
2.1.3 Software Piracy 06
2.1.4 Pornography 07
2.1.5 Credit Card Fraud 07
2.1.6 Telecommunication Piracy 08
2.1.7 Electronic vandalism, Terrorism, Extortion 08
2.1.8 Common Types of Cyber Attacks 09
2.2 Reasons of cybercrime 10
2.2.1 Capacity to store data in comparatively small space 10
2.2.2 Easy to access 10
2.2.3 Complex 10
2.2.4 Negligence 10
2.2.5 Loss of evidence 11
2.3 Profile of Cyber Criminals 11
2.3.1 Children and adolescents 11
2.3.2 Organized hackers 11
2.3.3 Professional hackers / crackers 12
2.3.4 Discontented employees 12
2.4 Victims of Cybercrime 12


Chapter 3

## IMPACT OF CYBERCRIME


3.1 Impacts against individuals 13
3.1.1 Harassment via e-mails 14
3.1.2 Cyberstalking 14

3.1.3 Pornography 15
3.1.4 Defamation 16
3.1.5 E- mail spoofing 16
3.1.6 Fraud & Cheating 17
3.1.7Computer vandalism 17
3.1.8 Transmitting virus/worms 17
3.1.8.1 Logic bombs 18
3.1.8.2 Trojan attacks 18
3.1.9 Web jacking 18
3.1.10 Internet time thefts 19
3.1.11 Intellectual Property crimes 19
3.2 Impacts against organization 20
3.2.1 Unauthorized control/access over computer system 20
3.2.2 Possession of unauthorized information 21
3.2.3 Software Pirate and Copyright 21
3.2.4 Financial Institutions are at risk 21

3.3 Impacts against the Government 22
3.3.1Cyber terrorism against the government organization 22
3.3.2 Trafficking 23
3.4 Conclusion 23

Chapter 4

**CYBER LEGISLATION AND LEGAL ISSUES- BANGLADESH PERSPECTIVE**

4.1 Cyber Tribunal 24
4.2 Cyber Appellate Tribunal 25

Chapter 5

**CYBER CRIME- INTERNATIONAL PERSPECTIVE**

5.1 Development of cyber laws in USA 26
5.2 Cyber related laws in Australia 27
5.3 Cyber related laws in Japan 27
5.4 Cyber related laws in Singapore 28
5.5 Cyber related laws in Malaysia 29
5.6 Cyber related laws in India 29
5.7 Cyber related laws in Pakistan 30
5.8 Cyber related laws in Nepal 31
5.9 Cyber related laws in Sri Lanka 31
5.10 Development of cyber law in Maldives 32
5.11 Cyber crime in Canada 32
5.12 Conclusion 32

Chapter 6

**SUGGESTIONS AND CHALLENGES**

**6.1 Suggestions to prevent Cyber Crime 33**
6.1.1 Constantly update passwords and login details 34
6.1.2 A secure computer will deter cyber criminals 34

6.1.3 Be social media savvy 34
6.1.4 Secure mobile devices 34
6.1.5 Protect personal Data 34
6.1.6 Be aware of what you do while using public Wi-Fi Hotspot 35
6.1.7 Protect the e-identity 35
6.1.8 Avoid being scammed 35
6.1.9 Secure the computer 36
6.1.9.1 Activate the firewall 36
6.1.9.2 Use anti-virus/malware software 36
6.1.9.3 Block spyware attacks 37
6.1.10Public Awareness 37
6.2 Challenges 37
6.2.1 General challenges 37
6.2.2 Legal challenges 38
6.3 Conclusion 40

Chapter 7

**CONCLUDING REMARKS**

7.1 Findings 41
7.2 Conclusion 43
BIBLIOGRAPHY 44

Chapter 1

# INTRODUCTION

## 1. Introduction

A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet. Along with the phenomenal growth of the internet has come to the growth of cyber crime opportunities.[1] Broadly stated, cyber crime can be said to be an act of commission or omission, committed on or through or with help of or connection with, the internet whether directly or indirectly, which is prohibited by the law and for which punishment, monetary and/or corporal, is provided.[2] But the existing penal or criminal laws are incapable to take action quickly to the rapid revolutions in Internet and computer network technologies. The consequence of crimes committed over the internet reach farther than traditional methods of committing crimes because there is no geographical boarder restrictions.[3] It is a new challenge for the law enforcers to prevent cyber crime by taking proper action. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications.[4]

## 1.2 Background

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 cybercrime 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.

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. There is sharp rise in the Cybercrimes in Bangladesh and the Law

---

[1] Michael Lee et al,. "Electronic Commerce, Hackers, and the search for Legitimacy: A Regulatory Proposal", 14 Berkeley Technology Law Journal, (1999), p.839.

[2] VivekSood, Cyber law Simplified, Tata McGraw-Hill:New Helhi,2001, p.37.

[3] Explanatory Memorandum, p. 6(acknowledging that criminals are often located in places other than where the harm occurred)

[4] http://www.legalserviceindia.com/articles/cyber.htm

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.

"February 6th, 7th and 8th of year 2000 were the days for cyber criminal and amongst the darkest nights ever for the Internet and e-commerce. Some of the big web-sites such as Yahoo, Buy.com, eBay, Amazon.com and E-Trade were chocked and shut down for hours.[5] Entering the millennium caused a huge disruption for companies due to a Denial of Service attack. Major web sites like MSN, Yahoo and Apache were shut down and hacked. The code red virus and Sircam virus spawned to millions of e-mail accounts worldwide. Cyber crime has only accelerated through the years, and has no plans to slow down.[6] It proves clear that cyber crime has a long history but in the present time it comes an alarming rate.

### 1.3 Problems

There is no doubt that cyber crime is one of the major problem in the present time. The law enforcers like the police or any other take it as a challenge to avoid cyber crime. Rapid developing of telecommunications and global computer networks has created the reasons, which allow to commit of cyber crimes in the high technologies field more easier. The telecommunication technologies opportunities use by criminal organizations very widely. 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 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.

---

[5] Cyber law simplified, op.cit.pp. 1 and 2

[6] Verton, Dan (2003). Invisible threat of cyber terrorism. New York. NY: McGraw-Hill/Osborne.

### 1.4 Objectives and Scope of studies

The overall purpose of the study 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:

(1) Types of cybercrime with the profile of cyber criminals and victims;
(2) Necessary Legislations in Bangladesh to tackle Cybercrime.
(3) To identify the challenges which should be taken to void Cyber crime.
(4) To find out the challenges of law enforcers to tackle cyber crime.

### 1.5 Methodology used

It is not possible to prepare a good research methodology without adopting a proper method. I have followed an analytical method. Applying this method I have collected the data from Secondary sources. As secondary sources, I have used the books of different writers, Newspaper, Journals and internet websites.

### 1.6 Hypothesis

Cybercrimes such as online hacking, software piracy, virus dissemination, child pornography, credit card fraud etcrepresent new crime methods, and continue to grow at an alarming rate. These create new and severe problems that are very complex to tackle. At the same time, they are engaging huge resources to hinder it.What challenges should be taken by the law enforcers to tackle cyber crime are mentioned in this research paper.

### 1.7 Duration of the studies

The research paper is made within two months fixed by the author for the partial fulfillment of the LL.M (1 Year) degree. I have tried my best to prepare a good research paper within that limited period of time.

### 1.8 Chapterization

Chapter One
Introduction
Chapter Two
Types of Cyber Crime with the profile of Cyber criminals, victims and resons
Chapter Three
Impact of Cyber crime
Chapter Four
Cyber legislation and Legal issues- Bangladesh Perspective
Chapter Five
Cyber crime- International Perspective
Chapter Six

Suggestion and Challenges
Chapter Seven
Concluding remarks

**1.9 Conclusion**

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world. Further I all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrime. I would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

Chapter 2

# TYPES OF CYBERCRIME WITH THE PROFILE OF CYBERCRIMINALS, VICTIMS AND REASONS

## 2.1 Types of Cybercrime

As it is stated earlier that the crime which is occurred through computer is cyber crime. So there is no doubt that a large numbers of crime are occurred everyday through computer and that's are cyber crime. Cyber crime includes not only the hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating and corporate espionage etc.[7] Some numbers of cyber crime is mentioned below-

### 2.1.1 Hacking

The cyber law of Bangladesh has, however, given a different connotation to the term hacking. So we will not use to term "unauthorized access" interchangeably with the term hacking. Unauthorized access would therefore mean any kind of access[8] without the authorization of either the lawful title holder or the person in charge of a computer, computer system or computer network. This is the trickiest definition of the group and controversy has followed its use for decades. Originally, the term hacker had a positive connotation and it actually had nothing to do with computer systems. In 1946, the Tech Model Railroad Club of MIT coined the term to mean someone who applies ingenuity to achieve a clever result. Then, when computers came along, "hacker" took on the meaning of someone who would "hack" away on a program through the night to make it better. But in the 80s everything changed, and Hollywood was the catalyst. When the personal computers onslaught started invading our daily lives, it didn't take long for clever screen-writers to bring the black hat villains of the cyber world to the forefront of our collective consciousness, and they haven't looked back since.

They associated our deepest fears with the word hacker, making them the ones that unraveled our privacy, put our safety in jeopardy, and had the power to take everything from us, from our material possessions to our very identities. And they could do it all anonymously, by hacking away in a dark room by the dim light of a computer monitor's glow. Needless to say, right or wrong, it stuck! Even many professionals in the computing field today have finally, albeit grudgingly, given in to the mainstream meaning of the word. "Hacker" has thus become the catch-all term used when in fact it should be "cracker."

### 2.1.2 Virus Dissemination

A virus is a computer program that was written to purposely damage computer system.[9]It is a malicious program or code that attaches itself to another program file and can replicate itself and

[7] Federal law enforcements Response to internet hacking: Hearing of the commerce, justice, state and judicial subcomm. Of the senate appropriations comm. 106th Cong (2000).

[8] "access" is defined in section 3(a) of the ICT Bill,2005.

[9] http://www.tekmom.com/buzzwords/zdvirus.html.

thereby infect other systems. Just like the flu virus, it can spread from one system to another when the infected program is used by another system. The more interconnected the host is, the better its chances to spread.

The spread of a virus can easily occur on networked systems, or it could even be passed along on other media like a CD or memory stick when a user unwittingly copies an infected file and introduces it to a new system. A virus could even be emailed with an attachment. "Virus" is often incorrectly used as a catch-all phrase for other malicious programs that don't have the ability to self-replicate, like spyware and adware.

So it can be said that viruses are very dangerous that means they are spreading faster than they are being stopped, and even the least harmful of viruses could be fatal. For, example, a virus that stops a computer and displays a message, in the context of a hospital life-support computer, could be fatal. Even the creator of a virus cannot stop it once it is "in the wild". So, it is clear that virus dissemination is one of the main cyber crime to damage ones computer. It cannot be denied that virus is the most serious thing to destroy ones computer.

### 2.1.3 Software Piracy

The biggest legal problem affecting the computer industry is software, which is the illegal copying or use of programs.[10] Piracy happen by copying the software from its original floppy disks a or compact disks and copying certain types of software directly from the server or even exchange programs over their organizational e-mail system.[11]The modern piracy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communication piracy.[12]It's often said that the use of products infected with malware (a form of computer virus) can cause substantial productivity losses to manufacturers, businesses, and pose security risks and threats to the critical infrastructure of the government.

But according to a report on cyber crime by Truth Labs, 65 per cent of samples are found to have more than one category of malware - which can bring down an entire network and misused by hackers to create bots that can attack large networks including SCADA systems protecting national resources such as power grids and satellite communications.

The research found that indirect security threats also include users or organisations unknowingly becoming part of a larger nexus of anti-social elements funding and supporting illegal activities such as organised crime, money laundering, drug trafficking, cyber terrorism and other related risks and vulnerabilities.

---

[10] Introduction to computer, opo.cit. p. 453.

[11] Introduction to computer, opo.cit. p. 453.

[12] Universal Declaration of Human Rights, adopted and proclaimed by general assembly resolution 217A (iii) of December 10, 1948, available at http://www.un.org/Overview/rights.html.

The copyright of computer software is protected under the provisions of copyright Act,2000. Major challenges in the copyright law were introduced in 2004 and 2005. The amendments to the Copyright Act in 2005 included the definition of computer and computer programme.[13]

### 2.1.4 Pornography

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive. Pornography websites did not get registered under the existing laws of Bangladesh. Women are also the becoming the victims of cyber crime nowadays due to the absence of cyber law.[14]

Child pornography, images of children involved in sexual activities, is traded on the Internet around the clock. Child pornographers use the Internet's ease of distribution to sell their material to pedophiles (adults who are sexually attracted to children). In addition to purchasing child pornography, pedophiles also visit online chat rooms hoping to lure children into situations for sex. Luring or tricking a minor into sexual activity is prohibited. For example, chatting with a fifteen-year-old girl over the Internet, then suggesting a meeting is illegal conduct. Traveling to a minor's home to engage in sex after meeting by way of Internet chat rooms is also criminal activity that will be prosecuted.

The biggest challenge to law enforcement in child pornography cases is the anonymous nature of Internet communication. The offenses also occur at high speeds across the entire nation crossing many law enforcement jurisdictions. Generally seller and buyer are in different states or could be anywhere worldwide.

As in other Internet criminal activities, the coordination between state, local, and federal law enforcement officials is essential.

### 2.1.5 Credit Card Fraud

When dealing with cybercrime, an ounce of prevention is truly worth a pound of cure. Cybercrime in all its many forms (e.g., online identity theft, financial fraud, stalking, bullying, hacking, e-mail spoofing, information piracy and forgery, intellectual property crime, and more) can, at best, wreak havoc in victims' lives through major inconvenience and annoyance. At

[13] Section 14(2) of the Copyright Act, 2000.

[14] The Independent, no cyber law in place, RAB officials being trained on cyber crimes, Dhaka, May 17, 2005.

worst, cybercrime can lead to financial ruin and potentially threaten a victim's reputation and personal safety

If cyber offences and credit card fraud were included in official data the total number of crimes in England and Wales would be more than 40 per cent higher, the UK's official statistician has estimated, undermining claims that the country is becoming more law abiding.

During the past few years, crime in the UK has fallen rapidly from its peak in the mid-1990s, mirroring similar declines in the US and western Europe. But some criminologists believe the reduction in traditional offences, such as burglary and vehicle crime, may partly be a result of illegal activity migrating online into a variety of cyber scams.

### 2.1.6 Telecommunication Piracy

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistable to many.

This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (United States, Information Infrastructure Task Force 1995, 131).

The Software Publishers Association has estimated that $7.4 billion worth of software was lost to piracy in 1993 with $2 billion of that being stolen from the Internet (Meyer and Underwood 1994).

Ryan (1998) puts the cost of foreign piracy to American industry at more than $10 billion in 1996, including $1.8 billion in the film industry, $1.2 billion in music, $3.8 billion in business application software, and $690 million in book publishing.

According to the Straits Times (8/11/99) A copy of the most recent James Bond Film The World is Not Enough, was available free on the internet before its official release.

When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss.

### 2.1.7 Electronic vandalism, Terrorism, Extortion

As never before, western industrial society is dependent upon complex data processing and telecommunications systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm (Hundley and Anderson 1995, Schwartau 1994).

While this potential has yet to be realised, a number of individuals and protest groups have hacked the official web pages of various governmental and commercial organisations (Rathmell 1997).[15] This may also operate in reverse: early in 1999 an organised hacking incident was

[15] http://www.2600.com/hacked_pages/ (visited 4 January 2000).

apparently directed at a server which hosted the Internet domain for East Timor, which at the time was seeking its independence from Indonesia (Creed 1999).

Defence planners around the world are investing substantially in information warfare-- means of disrupting the information technology infrastructure of defence systems (Stix 1995). Attempts were made to disrupt the computer systems of the Sri Lankan Government (Associated Press 1998), and of the North Atlantic Treaty Organization during the 1999 bombing of Belgrade (BBC 1999). One case, which illustrates the transnational reach of extortionists, involved a number of German hackers who compromised the system of an Internet service provider in South Florida, disabling eight of the ISPs ten servers. The offenders obtained personal information and credit card details of 10,000 subscribers, and, communicating via electronic mail through one of the compromised accounts, demanded that US$30,000 be delivered to a mail drop in Germany. Co-operation between US and German authorities resulted in the arrest of the extortionists .

More recently, an extortionist in Eastern Europe obtained the credit card details of customers of a North American based on-line music retailer, and published some on the Internet when the retailer refused to comply with his demands.

Cyber extortion is a type of cyber terrorism in which a website, e-mail server, or computer system is subjected to repetitive rejection of service or other attacks by wicked hackers, who demand money in return for promising to stop the attacks. Fearing that such attacks may become the custom in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by war fighting military commanders in the future me out of the domain. Perpetrators characteristically use a scattered denial-of-service attack.

### 2.1.8 Common Types Of Cyber Attacks[16]

| **Attack Types** | ***%*** |
|---|---|
| Viruses, malware, worms, trojans | 50% |
| Criminal insider | 33% |
| Theft of data-bearing devices | 28% |
| SQL injection | 28% |
| Phishing | 22% |

[16]http://www.go-gulf.com/wp-content/uploads/2013/06/cyber-crime.jpg

| | |
|---|---|
| Web-based attacks | 17% |
| Social engineering | 17% |
| Other | 11% |

## 2.2 Reasons of cybercrime

Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like many forms of **hacking**, are uniquely related to computers. There are many reasons for committing cyber crime. The main reasons for committing cyber crime is stated below-

### 2.2.1 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 more easier. Yes it is true that a large number of data can be stored in a small space.

### 2.2.2 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. So it can be easily said that cyber criminals can easily access ones account and commit the cyber crime.

### 2.2.3 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. So from the above discussion it is clear that complexity is one of the reason for committing cyber crime.

### 2.2.4 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. Negligence has been cited as

the key reason for cyber security breaches.Sometimes simple negligence can give rise to criminal activities, such as saving a password on an official computer, using official data in a public place and even storing data without protecting it.

The cyber criminal can take advantage of such negligence and use it to obtain, manipulate and forge information. 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.

### 2.2.5 Loss of evidence

The law enforcement community is facing a new challenge today, in the form of information technology age in the wired world. Asking a computer wizard to upgrade our computers or the reporting of computer crimes may be easy but combating this crime and getting successful convictions still remains an uphill task for the present law regimes around the world. Countries are depending more every day on innovative information technology in administering almost every aspect of daily life, ranging from ID cards, credit cards to health records or the security and defense of its borders. Yet, nations are now also concerned about taking specific steps in protecting themselves from losses caused by cyber criminals who act anonymously and may not even be within the national borders .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.

## 2.3 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-

### 2.3.1 Children and adolescents

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the BalBharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

### 2.3.2 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 NASAas well as the Microsoft sites is always under attack by the hackers. The subculture that has evolved around hackers is often referred to as the

computer underground and is now a known community.[17] While other uses of the word *hacker* exist that are related to computer security, such as referring to someone with an advanced understanding of computers[18] and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning. In this controversy, the term *hacker* is reclaimed by computer who argue that someone who breaks into computers, whether computer criminal (black hats) or computer security expert (white hats), is more appropriately called a cracker instead.

### 2.3.3 Professional hackers / crackers

Their work is motivated by the colour 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 even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

A professional hacker is far above average for computer hackers. Most hackers like the one your dealing with are nothing more than novices who watched some video on youtube™ on how to hack an email. Unfortunately, these kinds of hacking attacks happen all the time and that is why you should hire a professional hacker.

### 2.3.4 Discontented employees

This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. They are mainly involved with the cyber crime. To avenge they normally hack the system of their employee.[19]

## 2.4 Victims of Cybercrime

In general, victims of cybercrime are:

i. Desperados and greedy people
ii. Gullible
iii. Unskilled and Inexperienced
iv. Unlucky people

Nearly two thirds (65 percent) of web users across the world have been the victim of cybercrime, says Symantec.

Artwork: Diego Aguirre According to the security firm's "Norton Cybercrime Report: The Human Impact," 58 percent of victims of cybercrime, which includes viruses and online credit card fraud, feel angry, while 51 percent said they were annoyed and 40 percent admitted to feeling cheated.

---

[17] Blomquist, Brian (May 29, 1999). "FBI's Web Site Socked as Hackers Target Feds". *New York Post*.
[18] The Hacker's Dictionary". Retrieved 23 May 2013.
[19] www.carnegiecyberacademy.com/.../cyberCriminals/operate.htm

Furthermore, 80 percent of web users don't believe the cybercriminals will be caught while only three percent believe they won't fall victim to crime online.

Just 51 percent of web users said they would change their online behavior if they became a cybercrime victim, while just 44 percent of those that have fallen victim reported the crime to the police.

Joseph LaBrie, PhD, associate professor of psychology at Loyola Marymount University, likened cybercrime to "getting ripped off at a garage -- if you don't know enough about cars, you don't argue with the mechanic. People just accept a situation, even if it feels bad."

On average it takes 28 days to solve a cybercrime at a cost of around $334 (£218). More than a quarter (28 percent) of cybercrime victims said the time it took to solve was the biggest hassle resulting from the crime.

"We all pay for cybercrime, either directly or through pass-along costs from our financial institutions," said Adam Palmer, Norton's lead cyber security advisor.

"Cybercriminals purposely steal small amounts to remain undetected, but all of these add up. If you fail to report a loss, you may actually be helping the criminal stay under the radar."

The Norton Cybercrime Report also revealed nearly half of all web users think it's legal to download a single music track, album or movie without paying, while 34 percent admitted they thought it was ok to secretly view someone else's e-mails or browser history.

**Cybercrime Victims By Gender**[20]

| ***Gender*** | **%age** |
|---|---|
| **Male** | 71% |
| **Females** | 63% |

Chapter 3

## IMPACT OF CYBERCRIME

Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in a number of different ways, both online and in the offline world. Cyber crime affects not only the individual or organization but also it affects the government. The impacts of cyber crime is as follows-

### 3.1 Impacts against individuals

Cyber crimes committed against people include various crimes like transmission of child-pornography and harassment through e-mail. The trafficking, distribution, posting, and

[20] http://www.go-gulf.com/wp-content/uploads/2013/06/cyber-crime.jpg

dissemination of obscene material including pornography constitute one of the most important cyber crimes known today. Cyber harassment is a distinct cyber crime.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.

### 3.1.1 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. 6 Brillions of e-mail message are exchanged throughout the world daily. E-Mail has become one of the most widely used communications service in the world. Anyone with an e-mail account can send message to other users of the Internet and to many networks connected to the Internet through gateways.[21]

The matter has become more urgent since an e-mail message was sent to Bengali daily ProthomAlo, 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 TariqueRahman and Bangladesh Nationalist Party (BNP) lawmakers. The police department took the mails seriously and decided to set up a cyber crime control unit, which will be the country's first policing unit against cyber crime. 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 mail for fun. As there is no nationwide computer infrastructure, no watchdog or security system has yet been developed in Bangladesh.

### 3.1.2 Cyberstalking

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.

Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. The internet mirrors the real world. That means it also reflects real life & real people with real problems. Although it is rare, Cyber stalking does occur. A cyber stalker does not have to leave his home to find, or harass his targets, and has no fear of physical violence since he believes he cannot be physically touched in cyberspace. He maybe may be on the other side of the earth or a neighbor or even a relative! And a stalker could be of either sex.

Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female, but sometimes men

[21] Peter Norton, Introduction to computer p.295.

are also stalked. The figures are more on assumed basis and the actual figures can really never be known since most crimes of such natures go unreported.

### 3.1.3 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. Downloading 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 BalBharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

In males, the most immediate effect of pornography is "large increase in total sexual outlets the same day attributed to masturbation" with most "of them found the experience moderately sexually arousing, enjoyable, and generally pleasant, but some reported being disgusted, ashamed, and shocked."

Pornography addiction is a purported behavioral addiction characterized by compulsive, repeated use of pornographic material until it causes serious negative consequences to one's physical, mental, social, and/or financial well-being. There is no diagnosis of pornography addiction in the current *Diagnostic and Statistical Manual of Mental Disorders* (the DSM-5). The DSM-5 considers such diagnosis and rejects it because "there is insufficient peer-reviewed evidence to establish the diagnostic criteria and course descriptions needed to identify these behaviors as mental disorders."

A 2014 review, found that high-frequency use of visual sexual stimuli "fails to meet standards of addiction", e.g. because it can reduce unhealthy behaviors. Scientists do, however, state that excessive pornography viewing can be unhealthy if it becomes problematic for an individual due to personal or social reasons, including excessive time spent viewing pornography instead of interacting with others. Individuals may report depression, social isolation, career loss, decreased productivity, or financial consequences as a result of their excessive Internet pornography viewing impeding on their social life.In a 2014 American Psychological Association (APA) article, Kirsten Weir stated, "It's not clear, however, whether pornography is the proverbial chicken or the egg. Does a person turn to pornography because he's already in an unsatisfying relationship? Or do women pull away and lose interest in sex when they discover their partner is spending quality time with adult film stars?"

Despite little evidence in the research literature for the existence of pornography addiction, an academic review notes that a large, lucrative industry promises treatments for "pornography addiction", which is alleged to have an attendant risk of erectile dysfunction. On the other hand, there are reports of clinical experience that men who watch large amounts of porn come to need more stimulation and aggressive porn in order to become sexually aroused.The impact of Pornography in the society are spreading in an alarming rate. It is high time to take necessary actions by the law enforcement agencies to prevent cyber crime like pornography.

### 3.1.4 Defamation

It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking 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.

The tort of cyber defamation is considered to be the act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace. This is commonly done through the Internet via websites, blogs, forums, emails and instant messaging, chat rooms and now in the social networking sphere. Defamation law in general describes the tort as "the issuance of a false statement about another person, which causes that person to suffer harm" (Larson) where libel is the written form and slander is spoken. Libel is typically the form addressed with cyber defamation because the Internet essentially receives the same protections as print and published media. The other elements applied to defamation include:

- The unprivileged publication of the statement to a third party
- If the defamatory matter is of public concern, fault amounts at least to negligence on the part of the publisher
- Perceivable damage to the plaintiff

Along with the core elements of defamation, the burden of proof is placed on the plaintiff in a case, damages are usually awarded monetarily and in the United States, truth is an "absolute defense" (Larson).

Cyber or online defamation is considered to be as, if not more harmful than defamation in the form of libel and slander in the brick and mortar, physical world. In some cases, the effects of online defamation could be exponentially worse than an offline incident due to the global nature of the Internet and the fact that the statements can be accessed by virtually anyone. In addition to this, the issue of anonymity online raises even more concern when dealing with defamation because the author or origin of the statements may be very difficult to trace depending on the medium.

Although there has been some debate over whether defamation on the internet should constitute slander, it does not seriously seem to have questioned that libel is the appropriate cause of action.[22]

### 3.1.5 E- mail spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. Recently spoofed mails were sent on the name of Mr.

[22] Devine Rowland, "cyberspace: a world apart?" 13th annual BILETA Conference: the changing jurisdiction, Trinity college, Dublin, 27 and 28 March 1998.

Na.Vijayashankar (naavi.org), which contained virus. RajeshManyar, 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. E-mail spoofing can also cause monetary damage. Certain web based e-mails address of the purported sender of the e-mails.

### 3.1.6 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 center, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony website. Metropolitan magistrateGulshan 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 ayear's probation.e-mail fraud is frequently used to commit financial crimes.

The person committing the crime understands that there is very little chance of him actually being identified.

### 3.1.7Computer vandalism

Vandalism means deliberately destroying or damaging property of another. It is "action involving deliberate destruction of or damage to public or private property".[23]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.Computer vandalism is a program that performs malicious function such as extracting a user's password or other data or erasing the hard disk. A vandal differs from a virus, which attaches itself to an existing executable program.

### 3.1.8 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. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. Almost brought development of Internet to a complete halt. It is also a self-replicating virus. Worms use parts of an operating system that are automatic and usually invisible to the users. It is common for worms to be

[23] "Oxford English Dictionary". Oxford University Press. Retrieved 2015-04-25.

noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.[24]When used in all capital letters, WORM is an acronym for write once, read many, an optical disk technology that allows to write data onto a disk just once.[25]

### 3.1.8.1 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). In a computer program a logic bomb, also called slag code, is programming code, inserted surreptitiously or intentionally, that is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.[26] Trojan horse present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes.[27]

### 3.1.8.2 Trojan attacks

This term has its origin in the word 'Trojan horse'. In software field this means an unauthorizedprogramme, which passively gains control over another's system by representing itself as an authorized programme. 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. A Trojan as this program is aptly called, is an unauthorized program, thereby concealing what it is actually doing.

Trojan is not so much destructive as virus of worms. Computer Trojans are malicious programs often used by hackers to attack target computers, usually to provide a backdoor into the system, but sometimes just to cause destruction. Similar to the wooden horse, a Trojan horse[28] program pretends to do one thing while actually doing something completely different.

### 3.1.9 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

---

[24] http://searchSecurity.com.techtarget.com/sDefamation

[25] http://www.webopedia.com/TERM/w/worm.html

[26] http://www.whatis.techtarget.com.

[27] David Icove, Karl Seger and William Vonstorch, computer crime: A Crime fighters Handbook, 1st Edition August 1995.

[28] IEEE, 63(9) : 1278-1308, September 1975.

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 goldfish was changed. Further a ransom of US $ 1 million was demanded as ransom. Thus web jacking is a process where by control over the site of another is made backed by some consideration for it. In all the places where it had been mentioned, they had replaced the word "gold fish" with the words "Piranhas".[29]

### 3.1.10 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. ColonelBajwa's case- the 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 cyber crime. In recent times, many Internet users have been getting calls from persons identifying themselves as Isp officials, asking about their password and offering new passwords. It is a fraudulent task. The callers are not anyone belonging to the ISPs. Once they get the password, the callers will be using it entailing huge bills on the unsuspecting customer. During the last few days some GrameenCybernet valued customers are getting calls from strangers asking them about their password and also offering new password.[30]

### 3.1.11 Intellectual Property crimes

Intellectual Property rights have come into question recently with the explosion of Wed technologies.[31] Intellectual property crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. Intellectual property consists of a bundle of rights. Any unlawful act by which the owners deprived completely or partially of his rights is an offence. The common form of IPRviolation 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.

The prevention and punishment of IPR violations is very low in proportion to the number of infringements. The government also sets a poor example by failing to account fully for software in its tenders. A number of American films, including film studios, manufacturers of consumer goods and software films have reported violations of their intellectual property rights. Bangladesh is a member of the world Intellectual property Organization (WIPO), and acceded to the Paris Convention on Intellectual Property in 1991. So it can be said that the impacts of Intellectual Property crimes are increasing day by day. The law enforcers like the Police or RAB

[29] Cyber Crimes- Technical Issues, loc.cit.
[30] http://www.citechco.net/
[31] http://www.action.org

of Bangladesh should keep their eyes close to prevent cyber crime like Intellectual Property Crimes.

### 3.2 Impacts against organization

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 cybercriminal networks through Internet have attacked our country's technology infrastructure. Recently, hackers interrupted the DSE transaction, which cost the small entrepreneurs dearly.

#### 3.2.1 Unauthorized control/access over computer system

This activity is commonly referred to as hacking. The Indian law has however given 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. A computer can also be the target of criminal activity, as seen when hackers obtain unauthorized access to Department of Defense sites. Theft of information stored on a computer also falls within this category. The unauthorized procuring of trade secrets for economic gain from a computer system places the computer in the role of being a target of the criminal activity.

A computer can also be tangential to crime when, for example, it is used as a storage place for criminal records. For example, a business engaged in illegal activity may be using a computer to store its records. The seizure of computer hard drives by law enforcement demonstrates the importance of this function to the evidence gathering process.

### 3.2.2 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 anADC and a joint secretary, and a Pharmaceutical company.

### 3.2.3 Software Pirate and Copyright

It is the unauthorized duplication, distribution or use of computer software -- for example, making more copies of software than the license allows, or installing software licensed for one computer onto multiple computers or a server.

Copying software is an act of copyright infringement, and is subject to civil and criminal penalties. It's illegal whether you use the copied software yourself, give it away, or sell it. And aiding piracy by providing unauthorized access to software or to serial numbers used to register software can also be illegal. Results of an anonymous experiment conducted on more than 4,800 students in SanDiego were presented at the American Psychological Association conference. It says that38 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. The law enforcers should take vital part to stop the crime like software pirate and copyright and they should take it as their challenge.

### 3.2.4 Financial Institutions are at risk

We've been seeing some much targeted threats towards financial institutions through spear phishing attacks. What this does is target someone that is working for that financial institution. The user is then tricked to click on a link and malicious software is downloaded. It then lies dormant and is able to capture information within the actual organization itself, and send that information to third parties elsewhere in the world.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 cybercriminal networks through Internet have attacked our country's technology infrastructure. Recently, hackers interrupted the DSE transaction, which cost the small entrepreneurs dearly. Cyber criminals are also using some of the same old ruses when it comes to stealing bank customers' data and credit card numbers, compromising personal accounts and committing corporate account takeover. Targeting financial institutions is a low-risk, high-reward area for cyber criminals. Rarely are they caught or prosecuted.

### 3.3 Impacts 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 www.expressindia.comit was said that internet was becoming a boon for the terrorist organizations.

#### 3.3.1Cyber terrorism against the government organization

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 using512-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". Another definition may be attempted to cover within its ambit every act of cyberterrorism. 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 –

(1) putting the public or any section of the public in fear; or (2) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or (3) coercing or overawing the government established by law; or (4) 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.

### 3.3.2 Trafficking

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey. Traffickers use computer and information technology as an effective communication tool. They use IRC chat rooms in which people from anywhere the world come together and chat with each other. Criminals use it for meeting co-conspirators.

A number of international legal instruments require States to take measures to protect children from abuse and exploitation, as well as engage in international cooperation in the investigation and prosecution of child abuse and exploitation crimes. A lack of consistent and appropriate legislation across countries globally, however, remains a major impediment to successful investigations and prosecutions. Individual states vary considerably in their definitions of child abuse and exploitation, and often cannot move fast enough to enact laws that keep pace with technology.

To address these challenges, the Study covers the main forms of ICT-facilitated child abuse and exploitation, including the creation and distribution of child pornography, plus the commercial sexual exploitation of children, cyber-enticement, solicitation and grooming, cyber-bullying, cyber-harassment and cyber-stalking; as well as exposure to harmful content.

This Study, one of UNODC's tools to help states prevent and combat cybercrime, is accompanied by a package of technical assistance which includes law enforcement and judicial training, activities for improved international cooperation and awareness raising tools.

## 3.4 Conclusion

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime from the cyberspace. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world. Further it cannot be denied that there is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrime. It can be concluded with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

Chapter 4

# CYBER LEGISLATION AND LEGAL ISSUES- BANGLADESH PERSPECTIVE

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 BangladeshTatha O JogajogProjuktyAin 2006 (Information and Communication Technology Act, 2006) 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 withcybercrimes.Addl. IGP Mr. N.B.K. Tripura in his speech on the occasion of inaugurating Regional Cybercrime Seminar held on 5 November 2007 at hotel Sheraton, Dhaka said that- A case study of a computer virus, released by a young hacker in early 2000, highlights the huge imbalance between the crime and the punishment caused by the lack of adequate legislative measures to deal with the issue (Wojciech, 2007).

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-

- Mischief of computer and computer system
- Alteration of source code of commuter
- Hacking in computer system
- Publication of false, indecent and defamatory statement or information in electronic form
- Access in reserve system
- False representation and concealment of information
- False electronic signature certificate
- Transmission of secrecy
- Disclosing electronic signature for cheating
- Committing crime through computer.

## 4.1Cyber Tribunal

According to section 68 of the Information and Communication Technology Act, 2006for 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 –upon the report of a police officer not below the rank of sub-inspector orb) 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 newspaper to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall have the same power, a Sessions Court empowered to apply in its original jurisdiction. Public prosecutor shall conduct the case on behalf of the Government. Tribunal shall conclude the trial within six months from the date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

### 4.2Cyber 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 iseligible 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.

It is clear that both cyber tribunal and cyber appellate tribunal takes vital steps to punish the offenders of cyber crime.

Chapter 5

# CYBER CRIME- INTERNATIONAL PERSPECTIVE

The history of cyber related legislations are the first wave of law reform in most western legal systems emerged in the field of privacy protection in the 1970s and 1980s[32]. Technologically highly developed countries, especially those in Europe and North America have cyber related laws and cyber crime laws to protect and save their privacy, computer network and Internet. Civil legislation were enacted to protect data against illegal access to computer system by the following countries: Sweden in 1973 and 1986; in the United states of America in 1974, 1980and 1984; the Federal Republic of German in 1977 and 1986; Denmark in 1978 and 1985; Australia in 1978 and 1987; France in 1978 and 1988; Norway in 1978 and 1987; Luxembourg in 1979,1982 and 1993; Iceland and Israel in 1981; Canada un 1982 and 1985; the United Kingdom in 1981,1984 and 1990; Finland in 1987, 1990 and 1995; Ireland in 1988; Japan in 1997 and 1988; The Netherlands in 1992 and 1988; Portugal in 1991; Belgium in 1992; Switzerland in 1992 and 1994; Spain in 1992 and 1995; Italy in 1978 and 1997; Greece in 1988 and 1997; and Malaysia in 1977.[33] This legislation was a reaction to new challenges of privacy caused by expanded possibilities for collecting, storing and transmitting data by new technologies.[34]

## 5.1 Development of cyber laws in USA

The intersaction of technology and law is controversial.[35] The first widespread proposal for computer crime legislation was a federal Bill brought in the United Sates Congress by Senator Ribikoff in 1977. Although the Bill was not passed, but this proposal created consciousness about cyber risk all over the world as a pioneer foremost.

Congress of USA has tried to prevent children from receiving online pornography by enacting legislation that proscribes it. Though there have been other congressional attempts toi regulate the transmission of certain types of content on the internet, two of Congress most important effort to keep children away from pornography have been the Communications Dicency Act of 1996 and the child online protection Act of 1998.[36]

While there is no Comprehensive U.S privacy Law there are numerous privace laws thar address particular uses of data. The driver's privacy Protection (DPPA)[37] Act-1994 regulates disclosure or resale of personal information contained in records maintained by state departments of motor

---

[32] Marc D. Goodman and Susan W. Brenner," The Emerging Consensus on Criminal Conduct in Cyberspace", UCLA Journal of law and Technolog. (n.p.). vol.3, 2002, fn 146.

[33] UlrickSieber, "Legal Aspects of Computer- Related Crime in the Information Society", COMCRIME Study Prepared for the European Commission, p. 19(jan. 1998), accessed on http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc.

[34] The Emerging Consensus on Criminal Conduct in Cyberspace, Ioc. Cit.

[35] http://www.bambooweb.com/articles/i/n/Internet.html

[36] Christopher T. Furlow, "Erogenous Zoning on the cyber-frontier", verginia journal of law and Technology, vol. 5, no.7, 2000, University of Verginia, par. 14, retrived from http://www.vjolt.net.

[37] 18 U.S.C 2721-2725

vehicles.[38] The right to fundamental Privacy Act[39] protects the financial privacy and most of the provisions pertinent to the privacy such a bank records. Fair credits Reporting Act[40]relates to the credit reports and credit bureaus. Video Protection Privacy Act[41] bars video stores from disclosing customers video choice. The family education right and Privacy Act[42] relates to the educational institution information records and its protection of privacy. The Employee Polygraph Protection Act[43] limiting employers ability to use polygraph. The Telephone Consumer Protection Act[44] limiting use of automatic dialing machines in telemarketing and unsolicited commercial faxes.

**5.2 Cyber related laws in Australia**

Australia has a varied collection of provisions that address situations related to cybercrime. Many provisions of the Commonwealth, State and Territory criminal laws are general enough to encompass a crime that is merely facilitated by a computer. In theory, a person who collects and uses credit card details through use of the internet has not committed anything more exciting than garden variety fraud, although they may be exposed to more specific offences concerning telecommunications interception.

A number of new provisions have been developed to address the unique investigatory challenges created by cybercrimes. For example, under the Crimes Act 1914 (Cth), the Australian Federal Police may be able to compel a person to provide a means of accessing data protected by encryption (and provide for an offence of failing to reasonably cooperate with such an investigation). In addition, the Crimes Act 1914 could lawfully authorize the commission of offences by the police in investigating crimes (a tool that some have argued is necessary for addressing online child pornography).

However, Australia has a mixed record of success concerning cybercrime, as the international nature of the internet and the adaptability of networks and software tools continues to challenge the effectiveness of traditional law enforcement approaches.

**5.3 Cyber related laws in Japan**

Since 1995, the Internet has been continuously growing up.[45] Due to such a big change, the Japanese National Diet has enacted many new laws and amended relevant existing laws relating

[38] Reno v. Condon, 528 U.S 141 (2000)
[39] 12 U.S.C 3401-3422
[40] 15 U.S.C 1681-1681t
[41] 18 U.S.C 2710-2711
[42] 20 U.S.C 1232g
[43] 29 U.S.C 2001-2009
[44] 47 U.S.C 227
[45]TakatoNatsui, "The Recent Cybercrime Legislation in Japan" Meiji Law Journal. Vol. 10, March, Japan 2003. P.2.

to the Internet and courts of Japan also have been battling with such new problems, which have taken place on the Internet. The Japanese government signed the European council Cybercrime Convension-2001 and WIPO Copyright Treaty -1996. For this purpose, most provisions in the Copyright law of Japan have already been amended in accordance with the related condition by WIPO Copyright Treaty- 1996. In 24 March 2003 the Minister of the Ministry of Justice consulted a legislative examination for some amendments of the Penal Code and some relevant criminal procedure law to address the Cybercrime Convention.[46]

The penal code of japan had been amended in 1987. The penal Code of Japan enacted in 1907 and it is apparent that there was no computer system and computer data at the time. The main reason of this amendment was to ensure a modern computerized business work by prohibiting any computer crimes, especially to protect safety electronic fraud transfer transaction and the integrity of computer programs and electronic data.

Japan's cyber crime legislation is contained in another two enactments, the Unauthorized Computer access Law and the Computer Crime Act. Article 1 of the Unauthorized Computer Access Law- 1999[47]declares purpose of this law as follows:

The purpose of this Law is, by prohibiting acts of unauthorized computer access as well as by stipulating penal provisions for such acts and assistance measures to be taken by the Metropolitan of prefectural Public Safety Commissions for preventing the recurrence of such acts, to prevent computer- related order that is realized by access control functions, and thereby, to contribute to the sound development of the advanced information and telecommunication society.

### 5.4 Cyber related laws in Singapore

Singapore's cyber law regime is commenced by the introduction to the Electronic Transactions Act in 1998. This Act sets the basic legislative framework for e- commerce and electronic transactions.[48] In drafting the Electronic Transaction Act, the follofing guiding principles were adopted.

1. The need to conform to international standards and international models in order to be integrated with the global e-commerce framework,
2. The need to avoid over regulation,
3. The need to be flexible and technologically neutral to adapt quickly to a fluid global environment,
4. The need for transparency and predictability in our laws.

The Electronic Transaction Act aims to deal with these significant issues and to produce the legal framework for electronic transactions in Singapore. It removes existing legal implements and

[46]TakatoNatsui, "The Recent Cybercrime Legislation in Japan" Meiji Law Journal. Vol. 10, March, Japan 2003. P.4.
[47] Law no. 128 of 1999 and effective from February 3, 2000 in Japan.
[48] Compilation of cyber laws (Singapore). "Salient Feature of Electronic Transaction Act 1998", retrieved from http://cag .nic .in / Singapore.htm on 30 May ,2004.

instills confidence in business and individual t engage in e-commerce. Singapore's cyber crime legislation emerges in the computer misuse Act which was revised in 1998.[49]

### 5.5 Cyber related laws in Malaysia

Just like other countries, Malaysia also is also involved in evolution of technology. Internet has become a necessities for everybody in business, communicate socializing and many more. Despite being a positive tool for users, there are some of irresponsible people that are using internet in negative way such as online fraud, identity theft, virus attack and hacking.

Therefore, Malaysian government has already taking a big step to overcome these problems by introducing a few acts of law that can be used for cyber crimes.

These are a list of statutes in Malaysia regarding the Cyber law.

- Communications and Multimedia Act 1998
- Computer Crimes Act 1997
- Copyright Act (Amendment)1997
- Digital Signature Act 1997
- Electronic Commerce Act 2006
- Electronic Government Activities Act 2007
- Payment Systems Act 2003
- Personal Data Protection Act 2010
- Telemedicine Act 1997
- Penal Code (including Chapter on terrorism & cyber-terrorism)
- Communications and Multimedia Content Code

A person shall be guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer, the access he intends to secure is unauthorized, and he knows at the time when he causes the computer to perform the function that is the case.[50]

### 5.6 Cyber related laws in India

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore). An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate. Minor errors in

---

[49] Singapore computer misuse Act(Cap. 50A. Rev.ed..1998), retrieved from http://www.lawnet.com.sg/freeaccess/CMA-Details.htm. On 15 january,2005.

[50] Section 3 of the Computer crimes Act, 1997.

the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002.

The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002.

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT. Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

The Communications Convergence Bill-2001 aims at promoting, facilitating and increasing the carriage and content of communications including broadcasting, telecommunication and multimedia in an orderly manner, which has its roots in German Information and Communication Services Act as well in the British White Paper Proposals.[51]

On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

### 5.7 Cyber related laws in Pakistan

To legalize and correspond to the elaborated electronic transaction, the government of Pakistan promulgated the Electronic transaction, the government of Pakistan promulgated the Electronic Transactions ordinance in 2002 with the purpose of recognize and facilitate documents, records, information, communications and transactions in electronic form and to provide for the accreditation of certification service providers.

The Electronic transactions Ordinance address to define certain offences such as hacking, virus related offences, violations of privacy of information and damage to the information system. The Pakistan cyber law ordinance fails to address obscenity, cyber fraud, intellectual property rights,

[51] Rodney D. Ryde. "The Communications Convergence Bill: a critical analysis", the ICFAI Journal of cyber law, August (2003).

consent filtering, censorship and Spamming. Section 32 of this ordinance makes international offenders liable like the cyber law of India.

The electronic transaction Ordinance has amended certain prevailing laws with purpose of establishing legal recognition to electronic forms and gives legal recognition to electronic signatures. As a consequence, the Quran-e-shahadat order, 1984 has been amended to allow electronic documents as evidence.

**5.8 Cyber related laws in Nepal**

Cyber Law in Nepal is another important area which is deal by Company Registration in Nepal as cyber law is connected to our day to day life and is the significant area of human life. The government of Nepal (House of Representatives) has approved the Electronic Transaction Act-2006. The law does not only legalize all sort of electronic transactions and digital signatures, it has undoubtedly implied the ways to run several computer-based mechanisms and penalize cyber crime.

Electronic Transaction Act, 2008 and Regulations are in place in Nepal to control the cyber business and to legalizing all electronic transactions and digital signatures.

Apart from that the act has formulated the terms of Comptroller of Certification Authority which is further divided into 12 sections and 80 clauses. For more effective it has assigned separate judicial body called IT Tribunal and Appellate Tribunal to keep an eye into all cases which are connected to computer and cyber crime. If anyone is found to be violating Cyber Law then he/ she is equally punished like other crimes. We cannot ignore that Internet has unlocked numerous opportunities for mankind but it is also true that from cyber crimes are also getting huge place in our lives. Sometimes it's so serious that it takes immense time to solve the problem. There is no doubt that technologies are being a crucial part of humans and it is our responsibility to deal with cyber security.

As far as e-Commerce is concerned , the IT Policy-2000 was promulgated under the sub heading "Promotion of e- Commerce and so forth" states that e-business, telemedicine, tele-processing, distant learning, among others, shall be promoted by making necessary arrangements to encourage e-Commerce; necessary legal infrastructure shall be created for the promotion of tele-medicine, distant learning, tele-processing and e-commerce; intellectual property rights shall be protected through the formulation of necessary laws related to the development of information technology.[52]

**5.9 Cyber related laws in Sri Lanka**

At the time up to 2003, Sri Lanka is yet to come up with any legislative provision relating to cyberspace and e-commerce. The Telecommunication Act,1991 was introduced to prevent unauthorized access and misuse of telecommunication systems and network.[53] The Sri Lanka

[52]Kishor Pradhan, "From 3 to 18 ISPs in Nepal", A country paper on development of e-Services in Nepal, the 12th AMIC annual Conference: E-Words: Governments, Business and Civil Society, November 6-7, 2003.

[53] Articles 17 and 19 of the Telecommunication Act,1991.

Telecommunication Regulatory Commission has responsibilities to regulate all electronic communication including the information super highway in Sri Lanka.[54]

Since the Sri Lankan courts refused to accept computer evidence until recently, it was very difficult to prove and win a case relating to computer technology. Therefore it was facilitated to accept the information generated by computers as evidence by the Act No. 14 of 1995. In 2003 the Sri Lankan parliament passed the Information and communication Technology Act-2003 to provide for the establishment of the national policy on information and communication technology and for the preparation of an action plan. Under this Act, the information and communication technology agency is in charge of the implementation of the national policy in both the public and the private sector.

**5.10 Development of cyber law in Maldives**

At this time, Maldives is yet to furnish any legislative provision relating to e-commerce or any other field relating to cybercrime. However, new regulations were being drafted in Maldives under the responsibility of the Ministry of Communication Science and Technology (MSCT) and the National Centre for Information Technology (NCIT) in cooperation with the business community.

**5.11 Cyber crime in Canada**

It is probably true that Canada is dreadfully behind in its preparedness for averting a major comprise to its systems, whether it be banking, air traffic control, defence, energy generation, or telecommunications. But changing the laws is not going to change that. The RCMP is falling behind because of the growing technology gap between them and the criminals. There are not many officers of the law or prosecutors who understand the technical aspects of computer crime and how illegal acts are committed. What is needed is education. Times have changed, and how crimes are committed has changed as well. If the officers of the law and the courts do not get up to speed on cyber crime now, they will have missed the chance to close that ever widening gap.

**5.12 Conclusion**

Cybercrime greatly affects individuals, businesses, and national security due to the pervasiveness of the Internet. Increasingly, cybercrime is emerging as a major crime type in the 21st century. In this paper, we have provided an overview of cybercrime and reviewed the current status of fighting cybercrime in different countries. We believe that different countries should work together and use legal, organizational, and technological approaches to combat cybercrime so as to reduce the damage to critical infrastructures and protect the Internet from being abused. Many countries around the world are promoting international measures to deal appropriately with cyber crime for the growth of telecommunications, computer network. It is clear that almost every countries adopted cyber law to tackle the cyber crimes. It is a new challenge for the law enforcers of all the country to prevent the cyber crime by taking necessary actions.

[54] Act no 27 of 1996, The Telecommunication Regulatory Commission was established.

Chapter 6

# SUGGESTIONS AND CHALLENGES

It has been reported that the Cyber Crime rates as recorded by the FBIs Internet Fraud Complaint Center in USA has shown an increase of 60 % in 2003 with over 120000 complaints having been registered.[55] While in Bangladesh there is no device to collect such statistics, but it can be said that the crime rate here is not insignificant. This negligence on the part of the top management of many ICT Companies is simmering below the surface at present and is likely to explode into a ball of fire and engulf many companies.

This chapter also showed that the matters are very challenging for the growth of uses of computer network and Internet as well as existing laws of Bangladesh access to computer network, Internet and other computers, e-mail spoofing, e-mail bombing, sending threatening e-mails, sending defamatory e-mail, sending bulk e-mail, data diddling, denial service of attack, spreading viruses or worms, financial crime with the help of computer, committed various theft with and through computer or Internet, web jacking, cyber pornography, sale of illegal commodities, online gambling, forgery (Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners), cyber stalking, Internet privacy and Software piracy.

It is a delightful matter for netizens of Bangladesh that the ICT Act, 2006 contains enoughprovisions to check cyber crimes, which are not covered by any existing law of the land. Specific punishments are provided for these offences in the Cyber Law of 2006.

## 6.1 Suggestions to prevent Cyber Crime

The government of Bangladesh has taken some initiatives to combat with cyber criminal and reduce cyber crime. Some measures are relating to law i.e., amendment of certain part of law and enacting new law, other measures are relating to practice i.e., set up, trained up law enforcing team, cyber crime unit, recruitment of police officer as computer savvy, trained up particularly the Rapid Action Battalion (RAB) officials etc.

Twenty RAB officials returned home from Malaysia after completion of a training course conducted by the Malaysian Police on cyber crime and another twenty RAB officials are currently undergoing training on computer application and maintenance at the American International University-Bangladesh, which is scheduled to be concluded on 4 August, 2005.' Although the existing trial systems prevailing all over the world are not exactly fit for trying this sort of criminal activities, the origin of any cyber crime as well as the criminal could be detected by the Internet protocol (IP) number of any suspected e-Mail or web address as the IP number is unique for every electronic address.[56]

[55] http://www.naavi.org/cl_03.

[56] The Independent, No cyber law in place, RAB Officials being trained on cyber crimes, Dhaka, May17,2005.

### 6.1.1 Constantly update passwords and login details

By changing your login details, at least once or twice a month, one can cut down his chances of being a target of cybercrime. Selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?). Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.

Keep your passwords in a safe place and try not to use the same password for every service you use online.

Change passwords on a regular basis, at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious with one of your online accounts, one of the first steps you can take is to change your password.

### 6.1.2 A secure computer will deter cyber criminals

Always be sure to activate your firewall settings. Furthermore, installing anti-virus and anti-spyware software will protect your computer from various forms of malware, viruses, Trojan horses and other malicious software used to obtain your personal details. If the computer is secured by a strong anti-virus it will take a vital role to prevent cyber crime. So, it is the duty of a computer user is to secure his computer with anti-virus to avoid cyber crime.

### 6.1.3 Be social media savvy

Make sure your social networking profiles (e.g. Facebook, Twitter, YouTube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is extremely difficult to remove. The passwords of the social networking profiles must be constantly change.

### 6.1.4 Secure mobile devices

More often than not, we leave our mobile devices unattended. By activating the built-in security features you can avoid any access to personal details. Never store passwords, pin numbers and even your own address on any mobile device. This creates a great chance to commit cyber crime.

### 6.1.5 Protect personal Data

Use encryption for the most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in a different location. By protecting personal data cyber crime should be prevented.

### 6.1.6 Be aware of what you do while using public Wi-Fi Hotspot

While these access points are convenient, they are far from secure. Avoid conducting financial or corporate transactions on these networks. Although it's unlikely that nosy hotspot neighbors will put your privacy at risk, you should be on the alert for the most serious hotspot danger: a cybercriminal. These technically savvy hackers have the tools, skills, and patience to work around the limited protection measures some hotspot hosts take.

With these security dangers lurking, protecting yourself at public hotspots becomes your own responsibility. Here are some things you can do to keep yourself safe:

- Be aware of your surroundings. Make sure no one is peering over your shoulder when you log into your operating system, email, IM, or other accounts.
- Never leave your laptop or handheld device unattended-not even for a moment.
- Don't allow your wireless card to automatically join the nearest network. Instead, manually select the hotspot when you connect.
- Make sure you're on a legitimate hotspot by checking with the host to confirm the network name and connection process.
- Turn off file sharing when you're using a hotspot, and try to minimize the amount of sensitive, personal data you store on your laptops and mobile devices. You can usually turn off file sharing from your operating system's network settings menu.
- Don't do your online banking or trading at a public hotspot. Save it for a more safe and controlled environment.
- Limit email and IM to casual communications. If you use IM or email at hotspots, never send anything that should not be made public. Consider setting up an extra Web-based email account to use at hotspots.
- Don't surf websites you wouldn't want a stranger to know you're viewing.
- Turn off your wireless card when you're not using it.
- Make wise computing decisions. Always avoid using hotspots for any type of important communication or transaction.

### 6.1.7 Protect the e-identity

Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).

### 6.1.8 Avoid being scammed

Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

One can avoid being scammed by:

• checking the relevant regulatory agency's website to see if the company you are dealing with is listed and regulated. You can even contact the regulator to verify whether the company is regulated;
• doing general searches (e.g. on Google) to see what information can be found about the company you are dealing with;
• only dealing with people you trust. Dealing with individuals you have never met carries a higher risk;
• getting independent advice before entering into a transaction, or getting a second opinion from a trusted friend;
• keeping paperwork safe. When entering into any new relationship ensure that you maintain good records of all paperwork you receive and keep records of all your meetings and conversations. This may not prevent you from being scammed but will assist in the event that you need to take any action.

### 6.1.9 Secure the computer

#### 6.1.9.1 Activate the firewall

Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.A firewall is software or hardware that helps prevent hackers and some types of malware from getting to your PC through a network or the Internet. It does this by checking the info that's coming from the Internet or a network and then either blocking it or allowing it to pass through to your PC.
A firewall isn't the same thing as an antivirus or antimalware app. Firewalls help protect against worms and hackers, antivirus apps help protect against viruses, and antimalware apps help protect against malware. You need all three. You can use Windows Defender, the antivirus and antimalware software that's included with Windows 8, or you can use another antivirus and antimalware app.

#### 6.1.9.2 Use anti-virus/malware software

Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.Even the most perfect antivirus utility can't protect you against a real-world terror attack. Malware may exist in a variety of forms, such as a file, a hidden file or a partially corrupted file; it can hide the mechanisms that initiate the virus, such as a start-up service or a registry item. In the worst-case scenario, the malware is working for a third party that aims to steal valuable information like bank account numbers or personal identifiers without calling attention to itself. With modern malware, it is usually not enough just to remove a single virus file. Instead, multiple location checks and virus scanning techniques are needed to completely remove the package of malware. Fortunately, you're much more likely to encounter things your antivirus can defend the from, such as drive-by downloads, Trojanized apps, or malvertising

attacks. Just be sure you keep your antivirus active and up to date: You wouldn't want a zero-day attack to slip past your protection.

#### 6.1.9.3 Block spyware attacks

Spyware refers to software that is installed on a computer without knowledge of the user. It can be used to track and monitor computer use to send to third parties for marketing purposes. Spyware programs can be a nuisance, as they can take up computer processing capacity, collect personal information and send pop up advertisements without permission. Through key loggers or taking screen captures or scanning hard drives, spyware can maliciously take personal information for criminal gain. There are several steps you can take to block spyware from your computer. Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

### 6.1.10Public Awareness:

This course is no less important than technological precautionary actions, because most of the time common people become the victims of cyber threats and millions of computers are crashed away. So if it is possible to aware the populace about the nature, possible impairment and the antidote of the threats, it would be more convenient to defeat cyber criminals as well as save the virtual world and government can play the crucial role here.

## 6.2 Challenges

Not only the Government of Bangladesh but also the Law enforcement agencies of Bangladesh like the police, RAB etc should take it as a challenge to prevent cyber crimes. Along with the phenomenal growth of the internet and computer network, has come the upsurage of cyber law related challenges in the cyber world. Cyber law covers laws relating to Electronic and Digital Signature, Computer crimes, intellectual property, data protection and privacy, Telecommunications laws, etc. Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law-enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation. This chapter focuses on the challenges of fighting cybercrime.

### 6.2.1 General challenges

The increasing number of Internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out rather easily, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed has not been modified.

Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users. However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce.

The investigation and prosecution of cybercrime presents a number of challenges for law-enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime, but also to draft adequate and effective legislation. This section has reviewed key challenges to promoting cybersecurity and areas where existing instruments may prove insufficient and the implementation of special instruments may be necessary.

Cyber crime has only accelerated through the years, and has no plans to slow down.[57] There is a sharp rise in the cyber crimes in Bangladesh and the law enforcement machinery is finding it really difficult to manage these technical crimes in Bangladesh. The use of new technologies brings not only massive benefits to the societies, but also provides the opportunity to commit new kinds of crimes of traditional crimes using new means.[58] By enacting proper laws regarding the protection of cyber crimes and by giving proper training to the law enforcement agencies like the Police, RAB, BGB or other law enforcement agencies the Government may generally take challenge to prevent cyber crimes. Modern period is the period of technologies and it is very easy to commit a crime by using those technologies and cyber crime is the main example and the law enforcement agencies must take the initiative to prevent cyber crime by taking necessary actions.

### 6.2.2 Legal challenges

**Challenges in drafting national criminal laws**

Proper legislation is the foundation for the investigation and prosecution of cybercrime. However, lawmakers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.

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

[57] Verton, Dan (2003). Invisible threat of cyber terrorism. New York.

[58] The working party on the protection of Individuals with regard to the Procession of personal data set up by directive 95/46/EC of the European parliament and of the council of 24 October 1995, Official Journal no. L281 of 23/11/1995.

cyber offenderscyber crime could be prevented. The law enforcement agencies should take it as a challenge to stop cyber crimes.

**Adjustments to national law must start with the recognition of an abuse of new technology** Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes.Cyber crimes are being committed by using new technologies and new legislation should by enacted in such a way that the law enforcement agencies could use new technologies to protect cyber laws and prevent cyber crimes.

**Identification of gaps in the penal code** To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences. The gaps of penal code should be identified and exhaustive punishment should be given for cyber crimes. It might seem logical to structure the discussion which follows around these categories, i.e., to examine crimes that can be prosecuted under existing laws, crimes that can be prosecuted if existing law is modified and crimes the prosecution of which requires the adoption of new, cybercrime-specific penal laws. That is not the best approach because such a categorization ignores the internal logic of any penal code's offense structure. The more appropriate way to proceed is by analyzing offenses according to the traditional, empirically derived categories into which they fall, e.g., "crimes against persons," "crimes against property," "crimes against morality," "crimes against the administration of justice" and "crimes against the state.[59] The sub-sections below analyze the need for cybercrime legislation-either new penal laws or the modification of existing penal laws-to address offenses falling into each of these broad categories.

**Drafting of new legislation** Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures. Drafting cybercrime legislation separately may result in significant duplication and waste of resources, and it is also necessary to monitor the development of international standards and strategies. Without the international harmonization of national criminal legal provisions, the fight against transnational cybercrime will run into serious difficulties, due to inconsistent or incompatible national legislations. Consequently, international attempts to harmonize different national penal laws are increasingly important. National law can greatly benefit from the experience of other countries and international expert legal advice.

**Increasing use of ICTs and the need for new investigative instruments** Offenders use ICTs in various ways in the preparation and execution of their offences. Law enforcement agencies need

[59] http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm.

adequate instruments to investigate potential criminal acts. Some instruments could interfere with the rights of innocent Internet users. If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries.

The ICT policy in Bangladesh states that the internet, internets and Extranets provide links between the components of a business and its customers, suppliers and other business partners both at home and abroad. The law enforcement agencies by using adequate instruments should prevent the cyber crimes and they should take it as their challenge.

**Developing procedures for digital evidence**Especially due the low costs compared to the storage of physical documents, the number of digital documents is increasing. Digitization and the emerging use of ICTs has a great impact on procedures related to the collection of evidence and its use in court. As a consequence of this development, digital evidence has been introduced as a new source of evidence. It is defined as any data stored or transmitted using computer technology that supports the theory of how an offence occurred. Handling digital evidence is accompanied with unique challenges and requires specific procedures.

One of the most difficult aspects is to maintain the integrity of the digital evidence. Digital data are highly fragile and can easily be deleted or modified. This is especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down and therefore requires special preservation techniques. In addition, new developments can have great impact on dealing with digital evidence.

The evidence of cybercrime acts is almost always in electronic, or digital, form. This data can be stored or transient, and can exist in the form of computer files, transmissions, logs, metadata, or network data. Obtaining such evidence requires an amalgamation of traditional and new policing techniques. Law enforcement authorities may use ‘traditional’ police work (interviewing victims or undercover visual surveillance of suspects) in some stages of an investigation, but require computer-specific approaches for other parts.

### 5.2 Conclusion

It can be said that the law enforcers faced a great problem to stop cyber crime and they take it as their challenge. The government may prevent cyber crime by enacting new cyber laws. If proper steps could be taken the cyber crimes should be tackled. The biggest challenges of the internet users and computer users are facing to combat the cyber crime, which is the main focus of the subject matter. The use of new technologies being not only massive benefits for societies, but also provides the opportunity to commit new kinds of crimes of traditional crimes using new means. It is high time to take new challenge by the law enforcers to prevent cyber crimes by taking necessary actions. If it is not taken it may occur serious harm to the society.

Chapter 7

# CONCLUDING REMARKS

## 7.1 Findings

Education is the most vital weapon for literacy, as such seminars and workshops should be organized from time to time with emphasis on cyber safety so that the individuals will learn to keep their personal information safe and youth will flee cybercrime.

The findings from the study shows that youths involved in cyber crime are either in tertiary institutions or have graduated from tertiary institution. The study therefore, recommends that curriculum which will include courses on cyber crime, cyber management and its prevention should be introduced to both tertiary and secondary schools to take care of the present social changes.

The study discovered that there is no legislation on cyber crime. It is recommended that the government should immediately enact a comprehensive law on cyber crime.

In order for legislation on cyber crime to be effective and efficient when enacted, there is need for government to empower graduates by providing employment. Government should make provision for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals no matter how intelligent and cunning they may be. For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb cyber crime, it is recommended that there is need for them to understand both the technology and the individuals who engaged in this criminal act.

The findings showed that cyber criminals lives in the society, as such, prevention of cyber crime requires the cooperation of all the citizens and not the law enforcement agencies alone. It is therefore, recommended that everyone should watch and report to law enforcement agencies, anyone who indulge in cyber crime. Cyber criminals caught are been prosecuted by government. It is recommended that cyber criminals' assets should also be confiscated by the government and the imposition of longer prison terms for cyber criminals. This will serve as deterrence to those youths who want to indulge in such crime.

The innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they can not only be well informed about the current trends in cyber crimes, but they will also have the knowledge about different forms of the said crimes and how the cyber criminals carry out their heinous activities, thus they can devise means of protecting their information from cyber criminals.

Internet users should be security conscious. Similarly, internet users should not provide personal or financial information to others unless there is a legitimate and assumed reason for that. They should not for instance, throw out papers works like cheques, bank and brokerage statements, old credit cards, drivers license, passports, receipts from ATM among other numerous documents which usually have personal data. The internet services providers should not just provide broadband connection to their subscribers especially the home users, but they should also monitor effectively what the subscribers are doing on the net, at what time and where. They should provide their customers, especially financial institutions and cyber cafes with well-guided security codes and packages in order to protect their information and soft ware from hackers and publishers.

## 7.2 Conclusion

Cybercrime is a persisting international evil that transcends national boundaries in a manner that renders this form of organized crime a global concern. Cybercrime may take several forms including online fraud, theft and cyberterrorism. It has been seen that amongst the major reasons that facilitate the perpetration of this crime is the globalization of technology and the revolutionary advancement of ICTs that have impacted on criminal activity. Broadband, wireless technologies, mobile computing and remote access, Internet applications and services, software and file transfer protocols are amongst the tools utilized by cybercriminals to commit their crime. The increasing proliferation in usage of technology assisted criminal activity and cybercrime merits further attention from the global community by enacting the necessary legislative provisions and implementing effective technological and enforcement tools that reduce ICT-facilitated criminal activities. By and large, it is submitted that cybercrime should be subject to a global principle of public policy that aims at combating and preventing this form of organized crime through raising global awareness and increasing literacy rates, coordinating legislative efforts on national, regional and global levels, and establishing a high level global network of cooperation between national, regional, and international enforcement agencies and police forces.

# BIBLIOGRAPHY

## Books


- Dr. Zulfiquar Ahmed, first edition, 2009Cyber Law in Bangladesh.
- The Penal Code, 1860 (Act No. XLV of 1860).
- The Information and Communication Technology Act, 2006.
- Report on Regional Cybercrime Seminar, Dhaka (2007).
- Boham and Haley (2002).
- Kumar Vinod – Winning the Battle against Cyber Crime.
- Kapoor G.V. - Byte by Byte.
- Mehta Dewang- Role of Police In Tackling Internet Crimes.
- Duggal Pawan – The Internet: Legal Dimensions.
- Monjur Kader: Criminology (Cybercrime)


## Websites


- www.lawteacher.net/criminology/essays/computer-crime
- www.en.wikipedia.org/wiki/cyberwarfare
- www.ists.dartmouth.edu/cyberwarfare.pdf
- www.digitalworld.org.bd/cyber-security-cyber-crime
- www.ngccd.org/pdfs/pubs/cybercrime
- www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3
- www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.
- http://media.hoover.org/documents/0817999825_69.pdf.
- : www.heise.de/newsticker/meldung/54746;
- www.cert.org/archive/pdf/counter_cyberwar.pdf.
- www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.
- www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.
- :www.article19.org/pdfs/publications/freedom-of-expression-and internetregulation.pdf.
- www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=112556 0437610&a=KArticle&aid=1171452755624.
- http://media.hoover.org/documents/0817999825_1.pdf.
- www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf.
- www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.
- www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.