Thesis Report

On

“Prevention of Cyber Crime in Bangladesh”

Submitted by :

Md. Farhad. Hossain
ID: MBA2401031052
Program: Master of Business Administration
Major: Finance
Sonargaon University (SU)

Submitted to :

Department of Business Administration
Sonargaon University (SU)
Submitted for the partial fulfillment of the degree of
Master of Business Administration



Sonargaon University (SU)
147/1, Green Road, Panthapath, Dhaka-1215, Bangladesh
Date of Submission: January 07, 2025

Thesis Report

On

“Prevention of Cyber Crime in Bangladesh”

Submitted by:

Md. Farhad. Hossain
ID: MBA2401031052
Program: Master of Business Administration
Major: Finance
Sonargaon University (SU)

Supervised by:

Md. Shahbub Alam
Lecturer
Department of Business Administration
Sonargaon University (SU)

Submitted for the partial fulfillment of the degree of
Master of Business Administration



Sonargaon University (SU)
147/1, Green Road, Panthapath, Dhaka-1215, Bangladesh
Date of Submission: January 07, 2025

Letter of Transmittal

January 07, 2025
Md. Shahbub Alam
Lecturer
Department of Business Administration
Sonargaon University (SU)

Subject: Submission of Thesis Report on Prevention of Cyber Crime in Bangladesh.

Dear Sir,

Here I've come to submit my thesis report, which is an essential part of the MBA program. It has been huge accomplishment for me to work under your supervision. This has nothing but a great pleasure to submit the thesis report on **"Prevention of Cyber Crime in Bangladesh".**

This report provided me with theoretical as well as practical experience. Here I tried my level best to write an effective report by putting my academic knowledge into practice in order to make the document factual and credible. During my thesis period I observed operational activities done in GNFL and that helped me to gather as much information as possible to complete this report. However, I will be obliged to clarify if there is any disagreement in this report.

I kindly request your assessment of this report. Your feedback would be greatly appreciated. Thank you for your time and consideration.

Sincerely Yours

Md. Farhad. Hossain
ID: MBA2401031052
Program: MBA
Major: Finance
Department of Business Administration
Sonargaon University (SU)

Certificate of Supervisor

I hereby confirm that the thesis report titled **"Prevention of Cyber Crime in Bangladesh"** has been created for the fulfillment of MBA program requirements at the Department of Business Administration, Sonargaon University (SU). The report was conducted by Md. Farhad. Hossain, with ID MBA2401031052, under my guidance. I assure you that the report and its contents will not be utilized for any other intentions.

Md. Shahbub Alam
Lecturer
Department of Business Administration
Sonargaon University (SU)

Declaration of Student

I am Md. Farhad. Hossain, a student in the Master of Business Administration program with ID MBA2401031032 at Sonargaon University. I want to sincerely state that the report titled **"Prevention of Cyber Crime in Bangladesh"** has been genuinely created by me. During the preparation of this report, I ensured full compliance with international copyright regulations. I also want to clarify that this report has not been submitted anywhere else for the purpose of obtaining a degree.

Yours Sincerely

Md. Farhad. Hossain
ID: MBA2401031052
Program: MBA
Major: Finance
Department of Business Administration
Sonargaon University (SU)

Letter of Authorization

I hereby confirm that the report titled **"Prevention of Cyber Crime in Bangladesh"** is a genuine effort by Md. Farhad. Hossain. The report was conducted under my guidance. I also affirm that, to the best of my knowledge, the content presented in this report has not been included in any other report that led to the award of a degree to any candidate earlier, whether in the same context or a different one.

Md. Shahbub Alam
Lecturer
Department of Business Administration
Sonargaon University (SU)

Acknowledgement

First and foremost, I want to thank the Almighty ALLAH for providing me with the strength to carry out my obligations and complete the report on time. This report would not have been feasible without the devotion and efforts of a number of Individuals as it is involved diverse field of knowledge and experience. As a result, it would be unjust to overlook some of them, given their significant contributions. I am grateful to Md. Shahbub Alam, Lecturer, Department of Business Administration, Sonargaon University's (SU) for her unwavering supervision during my organizational period for agreeing to supervise me during the thesis period. My gratitude goes to entire Business Administration Department, of Sonargaon University (SU) for arranging Thesis Program that helps to understand the real-life situation

Abstract

This research is based on cybercrime only. The governments across the world, police departments and intelligence units have started to react to cybercrimes. This study provides an overview of cybercrime and examines awareness in different respondents on the issue of cybercrimes in Bangladesh as well as emphasizes the severity of the problem and the urgent need to limit its impact worldwide. It is pertinent to mention that without creating a precise legal framework enabling law-enforcement agencies to identify cyber offenders and prosecute them it is almost impossible to prevent cyber- attacks and cybercrimes in Bangladesh. Here also described the internet uses and its bad impact. The process of combating cybercrime is described here and the implementations of laws are shown in it. This thesis is totally based on laws of our country. It also focuses the lacings of our laws and how to solve this problem; it also described. How to combat cybercrime and by which way; it also mentioned here. Describe the combating system, which is mentioned in our Acts. What is the scenario of our country; also shown in this. Bangladesh is not capable to combat it now; it is proved in this research and the way of overcome from this is also mentioned. We haveno any laws to combating cybercrime and why it is urgent to make it; also elaborate inthis research.

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

Abbreviation and Acronyms

AFP : Australian Federal Police

CD : Compact Disc

BP : Bangladesh Police

BTTB : Bangladesh Telegraph and Telephone Board

CID : Criminal Investigations Department

ICT : Information and Communication Technology

IOP : Investigations, Operations and Prosecutions

IRC : Internet Relay Chat

ROM : Read Only Memory

TEDS : Training and Executive Development Specialist

Sl No	Name of Contents	Page No
	Cover Page	-
	Cover Page	-
	Letter of Transmittal	01
	Certificate of Supervisor	02
	Declaration of Student	03
	Letter of Authorization	04
	Acknowledgement	05
	Abstract	06
	Abbreviation and Acronyms	07
	Table of Contents	08-09
	Chapter-01	
1.1	**Introduction**	10
1.2	What exactly is cybercrime	10-11
1.3	Historical Back ground of cybercrime in bangladesh	12
1.4	Chapterization	13
1.5	Conclusion	13
	Chapter-02	
	Aims and Methods of the study	
2.1	introduction	14
2.2	Literature Review	14-15
2.3	Statement of Problem	15-16
2.4	Aims and objectives of the study	16
2.5	Justification or Rational	17-18
2.6	Scope & Limitations	18
2.7	Methodology of the study	17
	Chapter-03	
	Different Types of Cyber crime in Bnagladesh	20
3.1	Types of cybercrime	20-22
3.2	Cybercrimes against Property	23
3.3	Cybercrime against Government	23
3.4	Cybercrimes against Socity At Large	24
3.5	Present Situation	24-26
	Chapter-04	
	Cyber Laws in Bangladesh	
4.1	Introduction	27
4.2	Information and Communication Technology Act, 2026	27-28
4.3	This Act Declared Following Activities are Cybercrimes	28
4.4	Limitations of the said Act	28-29
4.5	Digital Nirapotta Ain 2018	29-31

4.6	Cyber tribunal	31-32
4.7	Cyber appellate tribunal	32
4.8	Pornography Act 2012 & Child pornography	32-33
4.9	Penal code 1860	34
4.10	Bangladesh Telecommunication Act, 2001	34
4.11	Cyber crime Report	35-40
	Chapter-5	
	Challenges For implementation or Combating Cybercrime	
5.1.	National plan:	41-42
5.2.	Law makers on the basis of cyber	42
5.3	Law Ministry on the rasis of cyber	42
5.4	Public Awareness about cybercrime	43
5.5	Internet Based Education	44
5.6	Digital Security	44
5.7	Investigational Power and Investigational System	44-45
	Chapter-06	
	Findings, Analysis, Recommendation & Conclusion	
6.1	Introduction	46
6.2	Findings	46-47
6.3	Criticisms	47-49
6.4	Recommendations	49-53
6.5	Conclusion	54
	Bibliography	55

Chapter-01

Introduction

1.1 **Introduction:**

Cybercrime remains a low priority in Bangladesh, despite the growing use of computers and the internet, with over thirty million internet users. However, very few computer-related crimes are reported to the police. Bangladesh does not have a Computer Emergency Response Team (CERT), cyber police, or virtual police to deal with issues like hacking, computer abuses, or information security breaches. Although the country passed the Information and Communication Technology Act of 2006, which can impose up to 14 years of imprisonment or a fine of up to 10 million taka for cybercrimes, this law does not seem to be enough to effectively address the issue. As the government plans to invest millions of taka to develop a digital Bangladesh, preventing cybercrime should be a higher priority. A significant portion of the budget must be dedicated to ensuring cybercrime prevention. This chapter explores Bangladesh's current policies on preventing cybercrimes and offers recommendations for improvement.

1.2 What exactly is cybercrime?

*****Cybercrime refers to a broad range of harmful activities carried out using computers or the internet. These activities include illegal actions like stealing data, interfering with systems, or violating copyright laws.

*****In 1997, John Carlin wrote an article for **Wired Magazine** titled "A Farewell to Arms." While Hemingway's novel of the same name is about a soldier saying goodbye to weapons, Carlin's article introduced a different concept, focusing on the dangers of technology and the emerging threats of cybercrime.

[1] The Council of Europe Convention on Cybercrime

What he meant to say is that future wars won’t involve traditional weapons. Instead, they will be fought in a different way, and the type of conflict he predicted almost 20 years ago is the reality we see today.

• "Offenses are actions committed against an individual or group with a criminal motive, aiming to harm their reputation or cause physical or mental damage, either directly or indirectly, using modern communication tools like the internet (chat rooms, emails, message boards, or groups) and mobile phones (SMS/MMS)."

• "Cybercrime is causing significant financial losses in businesses. Last year, losses were over $100 million, and the number is rising as security breaches become an increasing threat to U.S. companies, banks, and even the government."

Cybercriminals are often referred to as hackers. However, the term "hacker" is now used so widely that it is applied to anyone who breaks into computer systems, which is not entirely correct. There's a difference between hackers and crackers, though the term "cracker" isn't as common.

Hackers are people who access computer systems without permission, often just for the challenge or fun of it. They enjoy testing security systems and may believe they’re helping by finding weaknesses. These hackers don’t seek financial gain. On the other hand, crackers are people who break into systems for illegal reasons, such as stealing money, shutting down devices, pirating software, or altering or destroying data. Crackers often sabotage the victim's resources. Hackers are called 'white-hat hackers' (non-malicious), while crackers are called 'black-hat hackers' (malicious).

[2] Dr. Debarati Haldar and Dr. K. Jaishankar
[3] Beth Wilson

1.3 Historical Background of Cybercrime in Bangladesh:

Bangladesh, despite being a developing country, has experienced a rise in technology use. Many young people have easy access to computers and other devices, which gives them the chance to engage in hacking. Hacking has become a serious problem in the country, with many teenagers trying it out for fun. Even the media has often been involved in hacking and leaking private information.

One of the most well-known cybercrime cases in Bangladesh is the **Mahmudur Rahman** case. **Mahmudur Rahman,** the founder of a Bangladeshi newspaper called **Amar Desh**, was sued in December 2012 for publishing a report about a Skype conversation between Justice Md Nijamul Huq, the chairman of the International Crimes Tribunal, and a legal expert living abroad. He was sued along with the publisher of **Amar Desh**, Hashmat Ali, under a directive from the High Court.

Another notable incident occurred on February 15, 2012, when a group of Bangladeshi hackers called **"Black Hat Hackers"** attacked over 25,000 Indian websites, including important ones like the Border Security Forces (BSF) website.

Cybercrimes also include spreading false or biased information, which can lead to violence. For example, in the 2012 Ramu violence in Cox's Bazar, someone created a fake Facebook account using a Buddhist name and posted a photo claiming the Quran had been desecrated. This post sparked anger among Muslims, leading to attacks on innocent Buddhists in the area, and many Buddhist homes and temples were destroyed.

This shows that cybercrime is a serious issue in Bangladesh, and new forms of it are happening every day. If not controlled, the situation could worsen and affect law and order in the country.

1.4 Chapterization:

The thesis is divided into six chapters as follows:

The first chapter provides an introduction to the study. The second chapter explains the goals and methods used in the research. The third chapter discusses the various types of cybercrime in Bangladesh. The fourth chapter focuses on the cyber laws in Bangladesh. The fifth chapter addresses the challenges in implementing or combating cybercrime. The sixth chapter presents the overall findings, analysis, recommendations, and conclusion.

1.5 Conclusion:

This research focuses on preventing cybercrime in Bangladesh, an important issue for our country. Since 1996, cybercrime has been on the rise and continues to surpass our legal frameworks. This analysis aims to address the problem and propose solutions in a clear and straightforward manner.

Chapter-02

The goals and methods used in the Thesis

2.1 Introduction

Everything in research has a purpose and a clear plan for how it will be carried out. This section is crucial as it covers the literature review, problem statement, aims and objectives, justification or rationale, scope, limitations, and methodology. These elements help define the direction and framework of the study.

2.2 Literature review:

The topic of cybercrime prevention in Bangladesh has become increasingly important as the use of the internet grows. Many people have their own understanding of cybercrime and its control, often based on their personal experiences. However, one important question is often overlooked: ***Who is responsible for controlling cybercrime in Bangladesh?*** Most definitions of cybercrime fail to address this fundamental issue, which is crucial in creating a clear framework for prevention.

Every day, numerous cybercrime cases are reported, and while some articles and studies discuss these crimes, very few address the need for a specific body or authority to manage them effectively. One of the few people to write about this in-depth is Sufi Faruq Ibne Abubakar. In his article, he highlights the importance of addressing cybercrime, especially in the context of Bangladesh's goal to become a "Digital Bangladesh." He states, "The concept of a Digital Bangladesh is welcomed by IT professionals and the general public. To make this a reality, the government must pay serious attention to the issue of cybercrime. Without this, like many other positive initiatives, the dream of Digital Bangladesh will fail." He further mentions that the "National Information and Communication Technology (ICT) Guidelines 2009" have already included cybercrime as a key issue, but to truly succeed, the Ministry of Information Technology, along with IT professionals and the media, must work together.

In Bangladesh perspective we have a law, based on cybercrime is ICT Act 2006 & Digital Nirapotta Ain-2008. However, these laws are not sufficient to fully control cybercrime in the country. There are gaps and weaknesses in these legal frameworks that need to be addressed. What is even more important is the need for a dedicated body or organization that is

responsible for monitoring and controlling cybercrime. Such an organization would help enforce rules and regulations, and provide clearer guidance on how to prevent cybercrimes.

The use of the internet has become a fundamental part of life for educated people around the world, including in Bangladesh. However, it's not just educated individuals who are engaging with the internet. Even people with little formal education are increasingly using the internet. Unfortunately, many of them don't know how to identify harmful websites or avoid getting involved in illegal activities online. Some may unknowingly engage in cybercrimes because they don't fully understand the risks or how to navigate the digital space safely. On the other hand, there are some individuals, both educated and uneducated, who knowingly participate in illegal activities on the internet.

In light of this, the question arises: What can be done to reduce cybercrime? The answer lies in creating a clear system of control. If there were an effective regulatory body with the authority to oversee internet usage, enforce rules, and educate the public on safe online behavior, it could help reduce illegal online activities. Stronger regulations for internet access, along with awareness campaigns to inform people about the dangers of the internet, would be key to fighting cybercrime in Bangladesh.

In conclusion, while cybercrime is a growing issue in Bangladesh, the existing laws and frameworks are not enough to control it effectively. There is a need for a dedicated body to oversee and manage cybercrime prevention, enforce stronger rules for internet access, and educate people about the responsible use of the internet. Only then can Bangladesh reduce the prevalence of cybercrime and move closer to achieving its vision of a safe, digital future.

2.3 Statement of problem:

To build a secure cyber environment, it is crucial to establish an organization that has a deep understanding of the internet and related technology issues. This research is vital for encouraging governments to create effective cybersecurity systems. One potential strategy is to require individuals to register for internet access using their national ID or birth certificate number. This would ensure that no one can create multiple identities across platforms like social media, government, or official sites, and all user activity would be monitored and recorded.

Additionally, it would be important to implement a system where any user who visits a flagged or suspicious website triggers an alert to a security agency, which could then take

immediate action to investigate and arrest offenders. This approach would make it easier to enforce cybersecurity laws and reduce cybercrime.

Research in this area is essential for creating a safer, more secure digital world.

2.4 Aims and Objectives of the Study:

This statement emphasizes that every problem often comes with its own potential solution. The main goal of this research is to find a solution to reduce cybercrimes in Bangladesh. To achieve this, it is important to raise awareness about cybercrime among the people. People need to understand how the internet and the online world work. Cybercrimes, or crimes committed against computers and the information on them, are becoming a growing concern in many countries. This study aims to explore whether people would use the Internet to report cybercrimes.

The main objective of the study is to raise awareness about cybercrimes and to find ways to prevent and control them. Additionally, the research will look into ways to improve Bangladesh's cyber laws. The study will also present arguments and provide links to academic resources to better understand the issue of preventing cybercrimes in Bangladesh.

Here’s a simplified version of your objectives related to cybercrime and cybersecurity in Bangladesh:

1. **Understand the importance of cybercrime** both in Bangladesh and globally.
2. **Identify the problems with current cyber laws** in Bangladesh and how they affect the control of cybercrime.
3. **Learn about the details of cybercrime** in Bangladesh.
4. **Increase the effectiveness** of the government and law enforcement agencies in fighting cybercrime.
5. **Find ways to reduce economic losses** caused by cybercrime.
6. **Understand the reasons behind the rise of cybercrime** in Bangladesh.
7. **Explore the current state of cybersecurity** in Bangladesh.
8. **Understand why people get involved in cybercrime** and how it affects cybersecurity.
9. **Learn how cybercrime impacts families and society**.
10. **Find ways to reduce cybercrime** in Bangladesh.
11. **Understand how men get involved in cybercrime**.
12. **Explore ways to protect important data and information** from hackers.

2.5 Justification or rational:

I understand that you are emphasizing the importance of creating a peaceful and secure cyber world, and you're suggesting that the steps to achieve this go beyond just research. Here's a more refined version of your message, outlining some practical steps for building a better and safer digital environment:

While research into cyber security can certainly help society move toward a peaceful and secure cyber world, more comprehensive initiatives are needed to create lasting change. These steps can not only ensure a safer digital space but also provide employment opportunities for the unemployed, addressing both societal and economic challenges.

Here are some key initiatives that could contribute to a better cyber world:

1. **Cybersecurity Education and Training**: By promoting education in cybersecurity, we can empower individuals with the skills necessary to protect themselves and others. This not only creates employment opportunities but also ensures a workforce capable of tackling emerging digital threats.
2. **Protecting Internet Users**: With the right tools and strategies, we can help users navigate the internet safely. This includes protecting personal data, preventing scams, and ensuring that individuals can find accurate information rather than falling victim to misinformation or fraud.
3. **Child Protection**: There is a critical need to ensure that children are safe from harmful content and manipulation online. Implementing parental control tools, educating young users, and enforcing stronger regulations can help make the internet a safer space for children.
4. **Social Media Safety**: Social media platforms play a central role in modern communication, but they also present risks, such as cyberbullying and data privacy issues. Strengthening regulations, increasing platform accountability, and improving user awareness can help create a safer online environment.
5. **Protection of Official Sectors**: Government and corporate sectors must strengthen their cybersecurity measures to safeguard sensitive data. Preventing hacking, data breaches, and other cyberattacks is crucial to ensuring the smooth operation of these institutions.

In conclusion, achieving a better cyber world requires more than just research. It involves comprehensive actions, from education and training to safeguarding vulnerable groups and

securing online platforms. By taking these steps, we can create a safer, more inclusive digital world for everyone.

2.6 Scope & Limitations:

The study focuses on the current situation of cyber-crimes in Bangladesh. Since cyber-crimes are broader than other crimes, the researcher will examine common offences that occur in Bangladesh and the preventive measures for them. The study will be limited to the existing laws in Bangladesh, along with relevant international laws. Due to time constraints and the unavailability of necessary documents about cyber-crimes in Bangladesh, the study's scope is limited to the mentioned time and location. Additionally, there are several challenges in conducting research in Bangladesh, including:

1. Lack of secondary data.
2. Limited interest from respondents.
3. Time constraints.
4. Limited surveys conducted.
5. Insufficient funding.
6. Students' reluctance to share their views

2.7 Methodology of the Study:

In this study, I used a quantitative research approach with a survey to gather data and descriptive statistics. The reason for choosing this method is that the survey results are meant to reflect the views of the entire population of the country.

Since the research is exploratory, the research questions were developed based on existing literature. These questions aim to explore the level of awareness about cybercrime among the respondents, identify the types of cybercrimes occurring in Bangladesh, and determine what actions should be taken to prevent cybercrime.

The main respondents for this study are working professionals who are knowledgeable about computer crimes and security issues in their organizations. These professionals include senior managers, IT administrators, and IT security consultants. To select the survey sample, simple random sampling was used.

Chapter-3

Different types of Cybercrime in Bangladesh

3.1 Types of Cybercrime:

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

Hacking: it is a criminal offense that involves unauthorized access to the computer systems of individuals or organizations. It compromises the security of the victim, potentially exposing sensitive and confidential information. As such, hacking is considered a punishable crime, and there are strict laws in place to deter such activities.

Cyber-defamation: The internet allows for the rapid spread of misinformation, just as it does with accurate information. Websites, especially forums and chat rooms, can host false or harmful content, as users often post without moderation. It is crucial to recognize the significant threat posed by misleading or false information. Defamation can severely damage a person's reputation and dignity, as online statements can be seen by a global audience.

Cyber-extortion: Cyber-extortionists are individuals who create malicious software and use it to threaten people or organizations. They demand money in exchange for not causing harm, such as exposing or destroying sensitive financial and security information. If their demands are not met, they may carry out the threat. These cyber-extortionists can be seen as the modern-day version of cyber-mafias.

E-mail bombing: E-mail bombing refers to the act of sending a large number of emails to someone's inbox, overwhelming their email account and causing it to crash. This is typically done with the intention of harassing or disrupting the victim.

Cyber-Terrorism: A Growing Threat

The term "cyber-terrorism" was coined by Barry C. Collin in the 1980s and is defined as the deliberate, premeditated attack on information systems, computer networks, software, and data. These attacks are carried out with the intention of causing violence or disruption, often targeting non-combatant groups or entities. Cyber-terrorism has the potential to inflict catastrophic harm on both individuals and entire nations.

For instance, during a crisis like the events of 9/11, cyber-terrorists could exploit vulnerabilities in emergency communication networks to wreak havoc. By hacking into critical systems, they could shut down communication lines, divert emergency personnel, issue false orders, or manipulate information, thereby exacerbating the situation and leading to even more casualties. Such scenarios highlight the alarming potential of cyber-terrorism to disrupt national security and public safety in unimaginable ways.

In response to this growing threat, the United States has established specialized units such as the FBI's Cyber Security Unit (CSU), dedicated to safeguarding the nation against cyber-attacks. These units work tirelessly to defend critical infrastructure, ranging from telecommunications and transportation networks to financial data systems. As the digital landscape continues to evolve, the ability to wage war through cyber means becomes more apparent, demonstrating that conflicts may be won—or lost—without a single bullet being fired.

Virus Dissemination Virus: This is malicious software designed to infect and spread to other software programs. It can cause data loss, slow down internet speed, damage hardware, and more. Examples include Trojan Horses, Time Bombs, Logic Bombs, and Rabbits.

Software Piracy: This refers to the illegal copying, distribution, or use of software, where unauthorized copies of original programs are made and shared.

Pornography: Pornography is a successful online product that uses deceptive marketing tactics and techniques to keep users engaged. These websites can be accessed easily, even by children, with just a click of a mouse.

Credit Card Fraud: To make an online transaction, you typically enter your credit card number on the vendor's website. However, if electronic transactions are not properly secured, hackers can steal credit card numbers and misuse them by pretending to be the card owner. This can lead to significant financial losses, with large sums of money being misappropriated from bank accounts. In some cases, individuals are arrested and charged for stealing and using other people's credit card information.

Sale of Illegal Articles: Illegal items such as narcotics, weapons, and wildlife are being sold online through websites, auction platforms, and email. Some auction sites are suspected of selling cocaine under the guise of money.

Online Gambling and Money Laundering: Online gambling has become a huge industry, with millions of websites offering various types of games and betting services. However, there are concerns that some of these sites might be involved in illegal activities, such as **money laundering**. Money laundering is the process of concealing the origins of illegally obtained money, often by making it appear legitimate. While it hasn't been definitively proven that these gambling sites are directly connected to drug trafficking, there is suspicion due to the large sums of money being funneled through these platforms, which could be exploited for criminal purposes.

Intellectual Property Crimes: These are crimes that involve the unauthorized use or theft of intellectual property (IP), including **software piracy**, **copyright infringement**, and **trademark violations**. IP theft is a major concern in the digital world, as technology makes it easier to reproduce and distribute pirated software, counterfeit products, or steal computer code. These violations not only hurt the creators financially but can also undermine innovation and fair competition.

Cyber Defamation: Cyber defamation refers to the act of spreading false and damaging information about an individual or organization through digital means, such as social media, websites, or other online platforms. Defamation can seriously harm an individual's reputation or an entity's business standing. Since the internet provides a wide-reaching, anonymous, and fast platform for such actions, it is relatively easy for anyone to tarnish reputations, leading to potential financial, emotional, and professional damage. This is why cyber defamation has become a significant issue in the age of digital communication.

3.2 Cyber Crimes against Property:

As international trade grows rapidly, businesses and consumers are increasingly using computers to create, share, and store information electronically, replacing traditional paper documents. However, there are several offenses that can affect a person's property in the digital world. These include:

1. **Intellectual Property Crimes**: Infringement on patents, trademarks, copyrights, or other intellectual property.
2. **Cyber Squatting**: Registering a domain name similar to a trademark with the intent to sell it for profit.
3. **Cyber Vandalism**: Deliberate damage or defacement of websites and digital content.
4. **Hacking Computer Systems**: Unauthorized access or manipulation of computer systems and data.
5. **Transmitting Viruses**: Spreading harmful software or viruses that damage or disrupt computer systems.
6. **Cyber Trespass**: Unauthorized access to someone else's digital space or networks.
7. **Internet Time Theft**: Stealing or misusing someone’s online resources or time.

3.3 Cybercrimes against Government:

Cybercrimes against governments involve illegal activities carried out by groups aiming to threaten national or international security using the internet. These crimes include:

- **Cyber Terrorism**
- **Cyber Warfare**
- **Distribution of Pirated Software**
- **Possession of Unauthorized Information**

3.4 Cybercrimes Against Society at large:

An illegal action that harms cyberspace can affect many people. These crimes include:

- Child Pornography
- Cyber Trafficking
- Online Gambling
- Financial Crimes
- Forgery

3.5 Present Situation:

Charges were proven in only 15 out of 495 cases under the now-defunct Information and Communication Technology (ICT) Act, with conviction rates as low as 3% in cybercrime cases. Since the tribunal was established in February 2013, it was found that charges were proven in just 15 of the 495 cases, while 480 cases resulted in the accused being cleared of charges.

Out of the total cases, the police submitted final reports in only 129, and the accused were released due to lack of evidence. In 83 cases, the accused were discharged early when the court found the investigation reports to be flawed. In another 54 cases, the accused were acquitted because the prosecution failed to prove the charges. Most of the accused are released due to out-of-court settlements, a shortage of skilled lawyers, and law enforcement's lack of experience in handling cybercrime cases.

Cybercrimes continue to be reported daily, with 2,044 cases filed over the past six years. In 2018 alone, 925 cybercrime cases were filed, and 130 cases were reported in the first two months of 2019. The number of cases was only three in 2013, but it grew to 33 in 2014, 152 in 2015, 233 in 2016, and 568 in 2017.

[5] Cyber Tribunal (Bangladesh) in Dhaka
[6] Cyber Tribunal (Bangladesh) data

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

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

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

There aren't enough laws in Asian nation which can penalize the cyber criminals. In Bangladesh court there's a law named "The Bangladesh Information & Communication Law 2006" (Asamendedin 2009).Duringthis lawsection 56(1) hasdeclared thepenaltyoften years imprisonment with or while not fine.

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

Section sixty eight of the aforesaid act has declared the formation of a special court named "Cyber Tribunal".

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

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

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

But our government still not awake to the very fact. Web services provided through the native space network are liable to similar attacks and intrusions by hackers a lot of usually once the protection level is insufficient. Currently every day in Bangladesh some individuals send malicious mail to completely different foreign commission and alternative VIPs that generally cause major problem for the police and additionally for the govt.

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

[9] The Financial Express (10 January 2008)

Chapter 4

Cyber Laws in Bangladesh

4.1 Introduction:

To promote e-commerce and the growth of information technology, the ICT Act of 2006 was created. It included provisions for punishing cybercrimes, with a maximum penalty of 10 years in prison, a fine of up to 10 million Taka, or both. Recently, the Parliament amended the ICT Act 2006 to increase the penalties for cybercrimes. The new penalties now include a minimum of 7 years in prison and a maximum of 14 years, along with a fine of up to 1 crore Taka, or both.

The Information and Communication Technology (ICT) Act, 2006 came in force on 8 October, 2006. Subsequently, the government amended the Act in 2008 and in 2009. For the better application of the Act, the government passed Information Technology (Certificate Authority) rules in 2010. But these laws alone are not enough. To face the challenges growing in cyber space it is essential to amend the existing laws such as the Penal Code 1860, the Evidence Act 1872, the Contract Act 1872 etc. It is hoped that these Acts will be modified in accordance with the demand of time.

4.2 Information and Communication Technology Act, 2006

Section 54(1) of the ICT Act, 2006 lists different crimes related to cyberspace. Section 54(2) says, "If someone commits any of these crimes, they can be punished with up to 10 years in prison, a fine of up to 10 lakh taka, or both."

Section 56 states: "If someone, with the intention of causing harm or knowing they are likely to harm the public or another person, does something that destroys, deletes, or changes information stored in a computer, or reduces its value or usefulness, or damages it in any way, they have committed an offense."

Here is a simplified version of the given legal text:

(a) If someone illegally accesses a computer, computer network, or any electronic system that does not belong to them, it will be considered a hacking offense.

(b) Anyone found guilty of committing a hacking offense under subsection (1) of this section can face a punishment of up to ten years in prison, a fine of up to one crore taka, or both.

4.3 This Act declared following activities are Cybercrimes:

- Unauthorized copying or downloading of data or databases
- Introducing viruses
- Damaging or disrupting computer systems and networks
- Blocking access for authorized users
- Assisting others in committing crimes
- Hacking into computer systems
- Tampering with computer documents
- Using electronic forgery to cheat or damage someone's reputation
- Using forged electronic records
- Publishing digital signature certificates for fraudulent purposes
- Confiscating computers or networks
- Publishing obscene content in digital form
- Misleading or hiding facts to obtain a digital signature certificate
- Violating privacy or confidentiality
- Publishing false digital signature certificates

4.4 **Limitations of the said Act**:

Critics have pointed out several limitations of the ICT Act, 2006, in Bangladesh:

1. The Act does not address important intellectual property rights like copyright, trademark, and patent rights related to e-information and data.
2. Although the Act impacts e-commerce and m-commerce, it does not mention electronic payments for transactions.

The law was meant to apply to crimes committed worldwide, but it's unclear how this will be practically implemented.

3. While spamming is a major problem in many countries, Bangladesh's Act does not include provisions to prevent spam.
4. The Act doesn't define "domain name" or address the rights and responsibilities associated with it, which is crucial in the internet world.
5. The law doesn't cover crimes committed using mobile phones.
6. The Act allows emails to be used as evidence, which conflicts with the country's Evidence Act, as emails are not recognized as legal evidence.

We hope the government will take the necessary steps to address these issues and create a safer, crime-free digital environment for everyone.

4.5 Digital Nirapotta Ain 2018

This Act is an upgraded version of the cyber-protection law of the country, and will replace some of the controversial provisions of cyber-security laws, like section 57 of the ICT Act 2006.Some basic features of the Digital Nirapotta Ain 2018-It recognizes and defines E-Commerce, E-Transactions. In section 4 of the Act illustrates the jurisdiction of the Act, which covers both persons within and beyond the borders of Bangladesh.[10] Section 5 says about constitution of a Digital Security Agency, who shall monitor and supervise the digital contents, communications mediums including mobile phones to prevent cyber-crime. This section also introduces Digital Forensic Lab and Bangladesh Cyber Emergency Incident Response Team (Bangladesh-

[10] *Section 4* of Digital Nirapotta Ain 2018

CERT).[11]Section 13 of the Act illustrates the Power of the DG of Digital Security Agency, where the DG can order a ban on communication in extra-ordinary situation (security breach or national-international threat) to any individual or service provider.[12] In that case, the person or service provider has to facilitate the interception, monitoringand decryption of the Computer or source. It says the Act illustrates the cybercrimes in form of Hacking, impersonation, violation of privacy and other ways, on the basis of section 15.[13]Section 15(5) of the Act says, any derogatory comments, remarks, campaign or propaganda in electronic media made by a person, institution or foreign citizen, against the war of liberation, The trial under Digital Nirapotta Ain 2018 shall be held on the same Cyber Tribunal that was established under the ICT Act 2006; the procedures of the Tribunal shall be similar as well – concluding the trial within 180 days.

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

[10]*Section 4* of Digital Nirapotta Ain 201

[11]*Section 5* of Digital Nirapotta Ain 2018
[12]*Section 13* of Digital Nirapotta Ain 2018
[13]*Section 15* of Digital Nirapotta Ain 2018
[14]*Section 15(5)* of Digital Nirapotta Ain 2018
[15]*Section 36* of Digital Nirapotta Ain 2018
[16]*Section 16* of Digital Nirapotta Ain 2018
[17]*Section 21* of Digital Nirapotta Ain 2018
[18]*Section 2* of Digital Nirapotta Ain 2018

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



4.6 Cyber Tribunal:

Section 68 of the Information and Communication Technology Act, 2006 states that the government should set up one or more cyber tribunals to handle cases under this law efficiently. These tribunals will only deal with offences covered by the Act. The government will decide the local jurisdiction for each tribunal. In consultation with the Supreme Court, the government will appoint a Sessions Judge or Additional Sessions Judge to serve as the judge of the Cyber Tribunal. A case will be brought before the Cyber Tribunal:

a) Based on a report from a police officer, at least a Sub-Inspector, or b) Based on a complaint filed by a controller appointed under the Act, or by another person authorized by the controller.

b) The trial procedure in the Cyber Tribunal will follow the guidelines in Chapter 23 of the Criminal Procedure Code, 1893 (related to trial procedures in a Sessions Court), as long as it aligns with the provisions of the ICT Act.

[19] The Daily Star, **Saturday,** November 30, 2019

If the accused is absconded, tribunal can try the case in absentia. In this case tribunal has to circular an order in two Bangla newspapers to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall havethe 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 concludethe trial within six months from the date of framing charge. This period maybe extendedfor three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

4.7 Cyber Appellate Tribunal:

The government will establish one or more Cyber Appellate Tribunals, each consisting of a chairman and two members appointed by the government. The chairman must be either a former Supreme Court judge, an existing judge, or someone eligible to be appointed as a judge of the Supreme Court. One of the two members will be a retired District Judge or someone with judicial service experience, while the other will be an expert in information and communication technology. The members will serve for a term of 3 to 5 years.

The Cyber Appellate Tribunal will not have original jurisdiction but will only hear appeals from decisions made by the Cyber Tribunal and Sessions Court, in relevant cases. The decisions made by the Appellate Tribunal will be final, and it will have the power to modify, amend, or cancel the decisions of the lower courts. The tribunal will follow the appellate procedures similar to those of the High Court Division of the Supreme Court. Until the Cyber Appellate Tribunal is established, appeals will be heard by the High Court Division.

4.8 Pornography Act 2012 and Child Pornography

The **Anti-Pornography Act of 2012** in Bangladesh was enacted with the primary aim of protecting women, children, and adults from the harms of pornography, sexual harassment, and blackmailing, especially the distribution of sexually explicit material through mobile phones and other digital means. However, this Act is limited in scope, particularly when it comes to tackling the complex issue of cybercrime and child pornography in the digital space.

Key Points from the Act:

2.7.1 Definition of Pornography (Section 2):

The Act provides a legal definition of pornography, outlining it in the context of various forms of media. However, the definition does not extend explicitly to online content or cyber activities related to pornography, which is a major oversight given the rapid growth of internet usage.

1. **Investigation Procedure (Section 5):**

   Section 5 describes the procedure for investigating crimes under the Act, but it fails to specifically address how these crimes should be tackled in the digital world. It is more focused on traditional investigative methods, which may not be as effective in the rapidly evolving online environment.

2. **Production, Distribution, and Possession of Pornography (Section 4):** Section 4 criminalizes the production, storage, marketing, distribution, and display of pornography. While this is an essential step in addressing the issue, the law does not specifically cover online platforms or digital distribution methods, leaving gaps in regulation of the internet as a major channel for such crimes.
3. **Expert Opinion in Investigations (Section 7):**
   This section allows for the use of technical experts' opinions in investigations. However, the language is somewhat general and may not be fully adapted to the needs of modern digital investigations, especially with regard to cybercrimes involving online platforms.
4. **Offenses and Legal Procedures (Sections 10-11):**
   These sections detail that offenses under the Act are cognizable and non-billable, with procedures for investigation and prosecution in accordance with the Code of Criminal Procedure. While these sections lay out general legal processes, there is no clear reference to the unique nature of cybercrimes, which require specialized legal frameworks and digital forensic expertise.

[20] *Section 2* of Pornography Act 2012
[21] *Section 5* of Pornography Act 2012
[22] *Section 4* of Pornography Act 2012
[23] *Section 7* of Pornography Act 2012.
[24] *Section 10* of Pornography Act 2012.
[25] *Section 11* of Pornography Act 2012.

4.9 Penal Code 1860

The Penal Code of 1860 addresses traditional criminal activities such as theft, fraud, forgery, defamation, and mischief, which are also relevant to cybercrimes. However, with the rise of cybercrime involving the abuse of computers, the internet, and other digital technologies, new forms of criminal activity have emerged. These new crimes are often not fully covered by the Penal Code.

For instance, the Information and Communication Technology (ICT) Act of 2006 defines certain offenses that are not addressed by the Penal Code. Specifically, while the Penal Code contains a few provisions on cyber-related crimes like cyber-squatting, it lacks coverage for more complex cybercrimes such as hacking, internet time theft, and email bombing. This gap in the law suggests that the Penal Code alone is inadequate for controlling cybercrimes in the modern age.

Therefore, it is clear that to effectively combat cybercrime, the government must enact specialized laws that specifically address cyber-related offenses. These laws should be tailored to meet the unique challenges posed by digital technologies and ensure better regulation and enforcement.

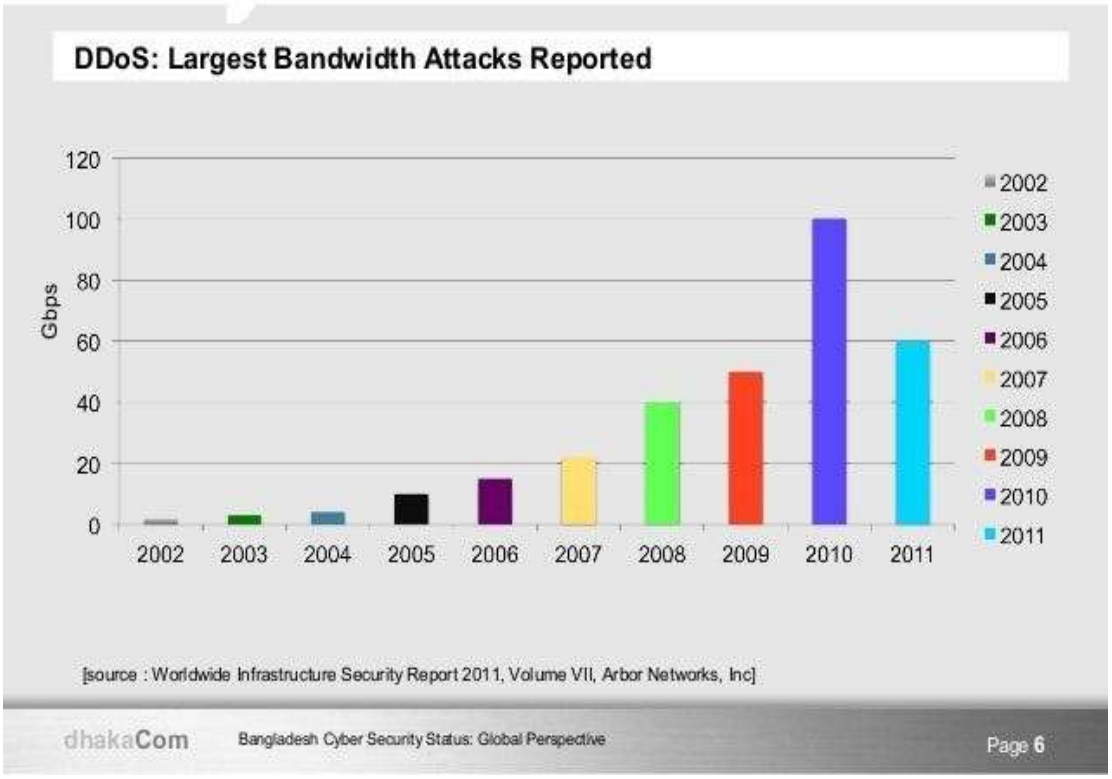
4.10 Bangladesh Telecommunication Act 2001

The Bangladesh Telecommunication Act of 2001 established a strong regulatory body for the telecommunications sector. Section 53 of this Act grants the authority the power to intercept communications in order to prevent any unwanted cyber incidents using telecommunication tools within the country. However, similar to the ICT Act, this section does not provide detailed information about cybercrimes. Instead, it offers a general description of various telecommunication services, including mobile, internet, telephone, fax, and others.

[26] *Section 53* of Bangladesh Telecommunication Act 2001.

4.11 Cyber Crime Report

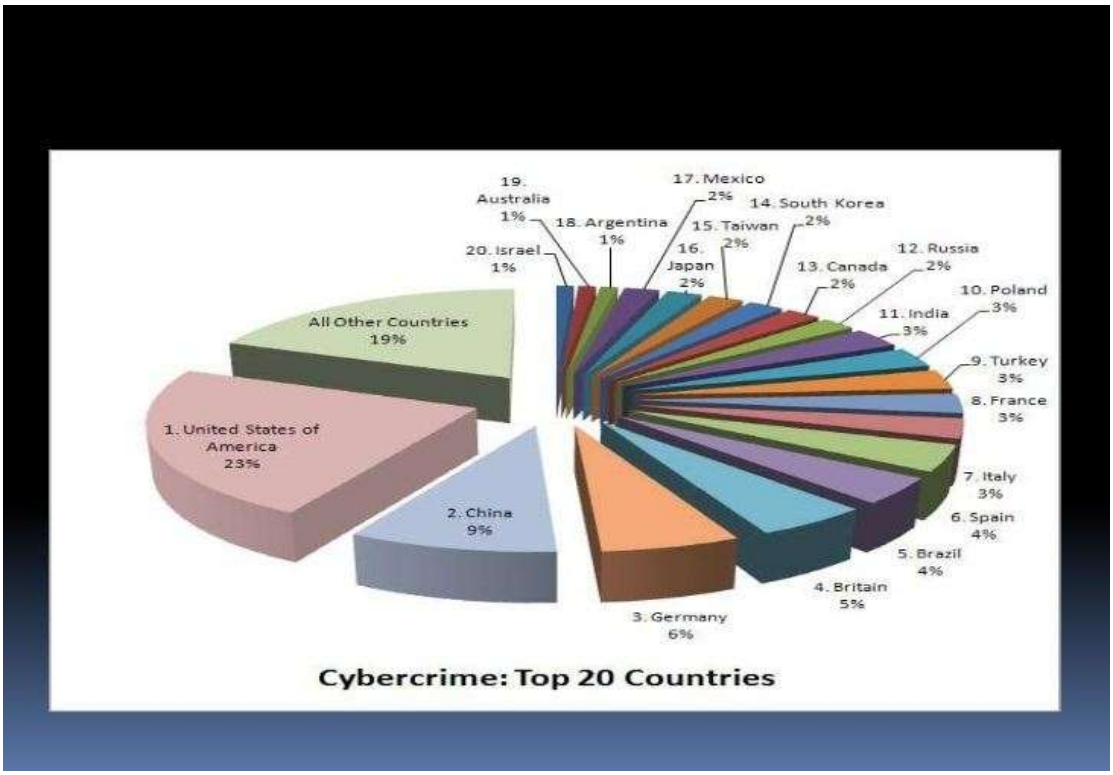
4.11.1 Global Security Statistics[27]



Based on the statistics from the picture, we can observe the trend of cybercrimes between 2002 and 2011. In 2002, the crime rate was below 1 percent per second. By 2003, the crime rate began to rise, and from 2004 to 2007, it increased rapidly, reaching around 20 crimes per second. In 2008, the rate doubled, reaching 40 crimes per second. In 2009, the increase slowed down, but 2010 saw a significant spike, with cybercrimes rising to 100 per second, marking a critical period in the cyber world. In response, global intelligence agencies took action, and by 2011, the crime rate decreased to less than 60 crimes per second.

[27]<http://www.slideshare.net/fakrulalam/bangladesh-cyber-security-status-in-global-perspective–[last visited on 21st >

4.11.2 Top 20 countries that commit the most Cyber Crimes[28]



1. United States of America
Share of malicious computer activity: 23%
Malicious code rank: 1
Spam zombies rank: 3
Phishing web site hosts rank: 1
Bot rank: 2
Attack origin rank: 1

2. China
Share of malicious computer activity: 9%
Malicious code rank: 2
Spam zombies rank: 4
Phishing web site hosts rank: 6
Bot rank: 1
Attack origin rank: 2

3. Germany
Share of malicious computer activity: 6%
Malicious code rank: 12
Spam zombies rank: 2
Phishing web site hosts rank: 2

[28]< http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/> –(last visited on 21st).>

Bot rank: 4
Attack origin rank: 4

4. Britain
Share of malicious computer activity: 5%
Malicious code rank: 4
Spam zombies rank: 10
Phishing web site hosts rank: 5
Bot rank: 9
Attack origin rank: 3

5. Brazil
Share of malicious computer activity: 4%
Malicious code rank: 16
Spam zombies rank: 1
Phishing web site hosts rank: 16
Bot rank: 5
Attack origin rank: 9

6. Spain
Share of malicious computer activity: 4%
Malicious code rank: 10
Spam zombies rank: 8
Phishing web site hosts rank: 13
Bot rank: 3
Attack origin rank: 6

7. Italy
Share of malicious computer activity: 3%
Malicious code rank: 11
Spam zombies rank: 6
Phishing web site hosts rank: 14
Bot rank: 6
Attack origin rank: 8

8. France
Share of malicious computer activity: 3%
Malicious code rank: 8
Spam zombies rank: 14
Phishing web site hosts rank: 9
Bot rank: 10
Attack origin rank: 5

9. Turkey
Share of malicious computer activity: 3%
Malicious code rank: 15
Spam zombies rank: 5
Phishing web site hosts rank: 24
Bot rank: 8
Attack origin rank: 12

10. Poland
Share of malicious computer activity: 3%
Malicious code rank: 23
Spam zombies rank: 9
Phishing web site hosts rank: 8
Bot rank: 7
Attack origin rank: 17

11. India
Share of malicious computer activity: 3%
Malicious code rank: 3
Spam zombies rank: 11
Phishing web site hosts rank: 22
Bot rank: 20
Attack origin rank: 19

12. Russia
Share of malicious computer activity: 2%
Malicious code rank: 18
Spam zombies rank: 7
Phishing web site hosts rank: 7
Bot rank: 17
Attack origin rank: 14

13. Canada
Share of malicious computer activity: 2%
Malicious code rank: 5
Spam zombies rank: 40
Phishing web site hosts rank: 3
Bot rank: 14
Attack origin rank: 10

14. South Korea
Share of malicious computer activity: 2%
Malicious code rank: 21
Spam zombies rank: 19
Phishing web site hosts rank: 4
Bot rank: 15
Attack origin rank: 7

15. Taiwan
Share of malicious computer activity: 2%
Malicious code rank: 11
Spam zombies rank: 21
Phishing web site hosts rank: 12
Bot rank: 11
Attack origin rank: 15

16. Japan
Share of malicious computer activity: 2%

Malicious code rank: 7
Spam zombies rank: 29
Phishing web site hosts rank: 11
Bot rank: 22
Attack origin rank: 11

17. Mexico
Share of malicious computer activity: 2%
Malicious code rank: 6
Spam zombies rank: 18
Phishing web site hosts rank: 31
Bot rank: 21
Attack origin rank: 16

18. Argentina
Share of malicious computer activity: 1%
Malicious code rank: 44
Spam zombies rank: 12
Phishing web site hosts rank: 20
Bot rank: 12
Attack origin rank: 18

19. Australia
Share of malicious computer activity: 1%
Malicious code rank: 14
Spam zombies rank: 37
Phishing web site hosts rank: 17
Bot rank: 27
Attack origin rank: 13

20. Israel
Share of malicious computer activity: 1%
Malicious code rank: 40
Spam zombies rank: 16
Phishing web site hosts rank: 15
Bot rank: 16
Attack origin rank: 22

By throwing in this picture we can realize that this is the statistics of world cybercrime ratings. On the basis of it is clear that United States of America gets the position 1st and23% of people are connected with this crime. At least 9% of people of China get attached with that sought of crime for that he got the position 2nd. Consistently, Germany 6%, Britain 5%, Brazil 4%, Spain 4%, Italy 3%, France 3%, Turkey3%, Poland 3%, India 3%, Russia 2%, Canada 2%, South Korea 2%, Taiwan 2%, Japan 2%

Mexico 2%, Argentina 1%, Australia 1%, Israel 1%, and the rest all countries are commit that types of crime totally 19%.

- On the rise[29]

Crime	2014	2013	2012
Facebook scams	120	87	72
Debit/credit card fraud	630	361	154
Lottery fraud	20	17	19
Email account hacks	65	41	74
Abusive calls/Msgs	58	46	50
Total cyber crimes	1,223	837	626

In Bangladesh, cybercrime has been rising steadily over the years. Here's a breakdown of the various types of cybercrimes and their trends:

- **Facebook Scams**: In 2012, 72 people were affected, which increased to 87 in 2013 and then to 120 in 2014.
- **Debit/Credit Card Fraud**: In 2012, 154 people were victims, rising to 361 in 2013, and reaching 630 in 2014.
- **Lottery Fraud**: There were 19 victims in 2012, which decreased to 17 in 2013, but then increased to 20 in 2014.
- **Email Account Hacks**: In 2012, 74 people were targeted, which dropped to 41 in 2013, and rose again to 65 in 2014.
- **Other Cybercrimes**: In 2012, 50 people were involved, which decreased to 46 in 2013.

Overall, the total number of cybercrimes increased from 626 cases in 2012 to 837 in 2013 and 1,223 in 2014. This shows a clear upward trend in cybercrimes, indicating that they are growing rapidly over time.

[29]<http://www.mid-day.com/articles/cyber-crime-doubles-in-navi-mumbai-in-2-years/15989157 –[lastvisited on 21st September,2016].>

Chapter 5

Challenges for Implementation or Combating Cyber Crime

5.1 National Plan:

It is very difficult to create a new law because the process is complex and involves multiple steps. First and foremost, we need to develop a national strategy to combat specific types of crime, such as cybercrime. The government must create a plan where all relevant stakeholders work together to address the threat of cybercrime.

Currently, the existing laws are insufficient, as they were not specifically designed to address cyber-related issues. To implement effective laws, we need to follow certain procedures, such as modifying existing laws or creating new ones that are more focused on cybercrime. This process will help ensure that the legal framework is clear and comprehensive.

5.1.1 Understanding the problem: First, we need to understand the problem at hand, especially the modern issues we face today. In today's world, everyone is deeply connected to the internet, which has led to the rise of crimes committed online. These internet-related crimes are no different from traditional crimes. Therefore, it's important to identify the different types of online offenses so that we can make informed decisions. However, when we look at our laws, it seems like there are no clear sections that help us understand or address these new challenges.

5.1.2 Partnerships and shared responsibility; individual crime: First, we need to understand the problem at hand, especially the modern issues we face today. In today's world, everyone is deeply connected to the internet, which has led to the rise of crimes committed online. These internet-related crimes are no different from traditional crimes. Therefore, it's important to identify the different types of online offenses so that we can make informed decisions. However, when we look at our laws, it seems like there are no clear sections that help us understand or address these new challenges.

Focusing on prevention: Our laws don't currently have any sections that focus on prevention. However, we need to set a goal to prevent this crime completely. If we are legally required to establish a clear target for prevention, this crime will eventually stop.

Balancing security freedom and privacy: The internet build on the freedom, creativity, and innovation of its users. While working to create a more secure online environment and combat cybercriminals, it is essential to balance the rights of users with national policies. Protecting individuals' right to privacy is crucial. Unfortunately, it is disappointing to note that such policy initiatives are not yet clearly outlined in our laws.

5.2 Law Makers on the Basis of Cyber:

In today's digital age, countries need to establish specialized bodies focused on cybersecurity and the internet. In our country, we currently don't have a dedicated organization to create laws specifically related to the internet. Instead, laws are made by individuals who may not fully understand the complexities of the digital world. This creates a problem because they can see the issues, but without a deep understanding of the internet, they may not know how to address them. As a result, the laws they create may not be effective or suitable. To solve this, we should create bodies made up of IT specialists, which would help in crafting appropriate and informed laws for the digital sector.

5.3 Law Ministry on the Basis of Cyber:

We currently don't have a dedicated ministry focusing specifically on cyber-related matters or the internet sector. However, in today's world, this is a significant issue, as many people are committing cybercrimes at an alarming rate, almost as if it were a natural part of society. The absence of a dedicated authority to oversee these matters leaves us vulnerable.

If the government were to establish a ministry for cyber issues, it would act as a guardian, protecting us from cybercriminals. Such a ministry would enable the creation of laws tailored to our needs and would involve scholars and experts in the field, ensuring that the laws are both effective and well-informed. This would be a crucial step towards creating a safer digital environment for everyone.

5.4 Public Awareness about Cybercrime

It's very important to educate people about all aspects of cybercrime. If they are not well-informed about these issues, they might unintentionally become involved in activities that could lead to cybercrime. Awareness and understanding of the dangers and rules around online behavior can help prevent people from making harmful mistakes.

"If we look at the situation today, we can see that there is a lack of awareness about cybercrime. Because of this, people are committing these types of offenses."

5.5 Internet Based Education

Today's children are the future, but our education system still relies heavily on traditional books. It's crucial to teach them about cyber-related issues as part of their lessons. Without this knowledge, they may unknowingly commit cybercrimes due to a lack of awareness. The government of Bangladesh should take responsibility for this by integrating cyber education into the curriculum. Laws alone are not enough; proper implementation is key to protecting society. Therefore, internet-based education is essential to prevent cybercrime.

5.6 Digital Security:

Our country lacks strong security, which has allowed criminals to hack our systems multiple times. If our security were stronger, these incidents would not occur. Although we have the Digital Security Act of 2018, it is similar to the ICT Act of 2006, and it is not enough to effectively combat cybercrime. We need to create a stronger security law. Otherwise, our country will continue to face harm and setbacks.

5.7 Investigational Power and Investigational System:

You raise an important point regarding the investigation of cybercrime and its distinct nature compared to other types of crime. While the laws may require at least a sub-inspector to handle investigations, the expertise required for cybercrime is far more specialized due to its technical and digital nature.

Cybercrimes often involve intricate IT systems, digital evidence, encryption, and online platforms, which makes it vastly different from conventional crimes like theft or assault. The standard investigative approach, which may work well for other types of crimes, is not adequate for cybercrimes. A sub-inspector or investigator with limited knowledge of technology may fail to understand the complexity of these crimes, leading to poor handling of crucial evidence, missed data, and incomplete investigations.

To address this issue, it would be beneficial to have investigators with a strong background in information technology (IT) and cyber law. Specialized training in digital forensics, data recovery, and online security would enable investigators to properly navigate the world of cybercrime and gather accurate, relevant evidence.

In some countries, there are already cybercrime units staffed with experts who handle cases involving hacking, data breaches, online fraud, and other digital offenses. These units follow specific protocols that prioritize IT systems and digital evidence handling to ensure that investigations are thorough and effective.

Ultimately, modifying the investigation procedures to take into account the unique characteristics of cybercrime is crucial. Cybercrime is not like traditional crime, and a one-size-fits-all investigative approach is insufficient. By incorporating experts in the field of technology and digital security into the investigation process, it would be possible to enhance the quality of the investigations and ensure that justice is properly served.

If the current investigative system does not reflect this, it may be necessary to advocate for reforms that introduce specialized training and units to deal with cybercrime more effectively.

Chapter 6

Findings, Analysis, Recommendation & Conclusion

6.1 Introduction:

In conclusion, this research highlights the need for stronger cybercrime laws and enforcement in Bangladesh. As the country rapidly develops digitally, with increasing numbers of internet users, the current security measures are inadequate. Cybercrimes such as bank fraud, the spread of inappropriate content, and the hacking of personal and public information are growing concerns. This research suggests that the government should establish a dedicated ministry and an independent body to address these issues, enforce cyber laws, and ensure security. Recent high-profile cases, such as death threats to political leaders, further emphasize the urgency of creating a proper legal framework and enforcement system. In short, Bangladesh must take immediate action to create and enforce comprehensive cyber laws to protect its citizens and digital infrastructure.

6.2 Findings:

It seems like you're pointing out two key issues with the Information and Communication Technology (ICT) Act of 2006, as related to addressing cybercrime. To make the language clearer and more concise, you might rephrase your findings as follows:

Problems Identified in Chapter Four:

Insufficient Provisions for Cybercrime: The Information and Communication Technology Act, 2006, does not adequately address the complexities of combating cybercrime. While the Act includes provisions relevant to cybercrime, these are not comprehensive enough to cover all modern challenges in the digital landscape.

Limited Scope of Relevant Sections: Only a few sections of the ICT Act, 2006, specifically address cybercrime. However, these provisions are not clearly defined or detailed enough to effectively combat the growing range of cybercriminal activities. There is a need to revise and expand the language of these sections for clarity and greater effectiveness.

Here is a simplified version of the text you provided:

- The punishment specified in the Information and Communication Technology Act, 2006, is not suitable for the types of crimes mentioned in the Act.
- Not all types of cybercrime are covered in the Act.
- The Act applies to all communication systems.
- To protect cyberspace, the government introduced the Digital Security Act, 2008, but it is essentially the same as the Information and Communication Technology Act, 2006, with no major changes.
- The Digital Security Act, 2008, describes what is considered lawful and unlawful access, but it is not very clear and is controversial.
- There is no section in the Act that specifies how to combat cybercrime.
- The Pornography Act of 2012 and the Child Pornography Act were created to protect cyberspace from pornography.
- These Acts do not cover all areas of cybercrime. For example, there is no solution provided for cybercrimes beyond pornography.
- The Penal Code does not specifically mention cybercrime but does describe similar offences in Section 13.
- The Bangladesh Telecommunication Act, 2001, only addresses issues related to cellular networks and does not cover modern cybercrimes. It is outdated and needs modification.

6.3 Criticisms

Where is our law? Where are our law makers? We have any sector of cybercrime? No, we haven't. We have also law but this is not basis on the cyber, we also have a huge number of scholars' law makers; but are they scholar in that sector? I think no, because this is a very new problem of our country. Perhaps it is new but we are seeking for a law on it. Because, it is a very dangerous problem. We want a secure store house of internet. We have no any individual ministry on the basis of this. We have no any proper education on it. We have to permit a compulsory subject on it to our education to aware about cybercrime.

6.3.1 Critical Analysis:

It is rightly said that prevention is better than cure. It is always better to take certain precautions while operating the internet. As Bangladesh is a part of the wo

The country is emerging as both an economic and political power in the South-Asian region, with a GDP growth rate of around 6.5% in recent years, including 7.05% in 2016. It is also experiencing a cyber revolution under the slogan of Digital Bangladesh, with initiatives to provide computer and Internet access across the country, even in remote villages. However, with this rapid digital transformation comes the increased risk of cyber-attacks, particularly targeting the financial sector. Such attacks could severely damage not only the Internet infrastructure but also the country's economic stability and development, as demonstrated by the recent hacking of the Bangladesh Bank, where 80 billion US dollars were stolen. Cybercriminal activities, whether originating from within the country or abroad, have the potential to disrupt the country's economic, social, and political stability. Therefore, it is crucial that the people of the country become aware of these risks and take the necessary precautions to protect their online and digital activities. In this view one may keep in mind the followings:

1. Children should avoid sharing personal details like their names, address, school, and phone number in chat rooms. They shouldn't send pictures to anyone and should ignore rude, threatening, or inappropriate messages. They must remember that people online may not be who they say they are.
2. Parents should use software to block harmful content like pornography, gambling, drugs, and alcohol on their computers. They can also set time limits on internet use and check which websites their children visit.
3. People should back up their data regularly to avoid losing important files if their computer gets infected with a virus.
4. It's important to use up-to-date antivirus software to protect your computer from viruses.
5. Never send your credit card information to a website unless it's secure.
6. If you encounter something harmful online, don't panic. If there's immediate danger, contact the police. Avoid getting into arguments or sharing too much personal information with strangers online.
7. Be careful when meeting people you've only met online. Keep a record of your conversations as proof, and don't alter the messages.
8. Large organizations should use firewalls to control access and ensure only authorized users can communicate with their internal network.

9. Passwords are important for protecting network systems. Always change your password regularly, and make sure it’s a combination of letters and numbers that’s hard for others to guess.
10. System managers should regularly check their network for vulnerabilities, bugs, and weaknesses before hackers can exploit them.

6.4 Recommendations:

6.4.1 Policies Recommended for Prevention of Cyber Crime in Bangladesh: Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bringing intopractical part so that the practices become easier to implement. Policies recommended are as follows:

Here is a simplified version of the text:

a. Effective information systems require integrated policies. A major challenge in developing a cyber-society is the shortage of financial resources and trained personnel.

b. A strong education system is essential, focusing on Information Technology (IT) at all stages of education. This IT should be secure, free from cybercrime, and accessible to everyone.

c. Promoting research and development in ICT and human resources should be a key part of the system.

d. There should be up-to-date and consistent cyber laws to address cybercrimes and protect intellectual property, creating a safer information society.

e. Adopting ICT standards, regulations, and quality assurance is necessary to ensure high-quality services and products, encouraging competition for the benefit of communities within each country.

Here is a simplified version of your article:

a. People in all parts of society need to be aware of information security and cybercrimes. There should also be more sharing of information on these issues at both the regional and national levels.

b. There should be effective ways to detect and prevent cybercrimes, especially at local levels, to protect against and respond to these crimes.

c. National awareness campaigns should be conducted for everyone, including children, students, government workers, and private sector employees, using various media platforms.

d. The government should work with media professionals to educate them and encourage them to spread awareness to the public.

e. Large private companies and industry groups should support awareness programs.

f. More focus should be given to less developed countries to create better systems for protecting against and responding to cybercrimes.

g. Efforts should be made to promote tools like filtering, parental controls, and software that helps create a safe online environment for children.

h. Police should be trained and equipped to handle high-tech crimes. Laws should allow for the quick gathering and access to electronic data, which is often key to solving crimes.

i. Countries should have systems in place for sharing evidence quickly in cases of international cybercrimes.

j. There should be a network of knowledgeable experts to respond quickly and effectively to international cybercrimes, with a contact person available 24/7.

k. The government should support outsourcing to create a team of virtual police officers and set up cybercrime police stations across the country. These officers should receive specialized training, both locally and internationally.

l. Raising awareness, educating people, and providing technical support to prevent online crimes is important, but this should not stop the growth of e-commerce.

Recommended for Cyber Crime Prevention in Bangladesh: Here is a simpler version of your article:

a. Everyone should know about information security and cybercrimes. People need to share information about these issues in their communities and across the country.

b. There should be ways to find and stop cybercrimes, especially at the local level, to protect people and deal with these crimes.

c. National awareness campaigns should be made for everyone, including kids, students, government workers, and private employees, using TV, radio, and social media.

d. The government should work with the media to help teach people about these issues and encourage them to spread the word.

e. Big companies and industry groups should support programs to raise awareness.

f. More focus should be given to poorer countries to help them build better systems to stop and handle cybercrimes.

g. Tools like filters, parental controls, and safety software should be used to keep children safe online.

h. Police need special training and equipment to deal with cybercrimes. Laws should allow them to quickly get and use electronic evidence to solve crimes.

i. Countries should have systems to quickly share evidence in international cybercrime cases.

j. There should be a team of experts available 24/7 to handle international cybercrimes.

k. The government should create virtual police teams and set up cybercrime police stations across the country. These officers should get special training both locally and internationally.

l. It's important to raise awareness, teach people, and offer support to prevent online crimes, but this should not stop the growth of online businesses.

Here’s a simplified version of the article, using easier words:

1. Protecting Children: Always keep an eye on the websites children are visiting to make sure they are safe from any kind of harm or inappropriate content.

2. Secure Your Program: Use a security program that controls cookies (small files websites store on your computer). Leaving cookies unprotected can lead to security risks.

3. Watch Website Traffic: Website owners should regularly monitor traffic to spot any unusual activity. Installing security tools on servers can help with this.

4. Protect Your Internal Network: Web servers that run public websites should be kept separate and secure from the internal business network.

5. Backup Important Files: Make sure to back up your important files and folders regularly. This helps protect your data if your computer breaks down or is attacked.

6. Disconnect When Not Using: Disconnect from the internet when you're not using it to protect yourself from online threats.

Other Tips for Safe Internet Use:

Here’s a simpler version of your article:

- Keep your security software updated and make sure your browser and operating system are current.
- Turn off file sharing on your computer.
- Disconnect from the internet when you're not using it.
- Check your online accounts regularly to make sure everything is correct.
- Use different passwords for each account.
- Don’t reply to text messages from people you don’t know.
- Don’t share your phone number online.
- Be careful when opening email attachments.

6.4.2 Recommendations:

Here’s a simplified version of your article with clearer structure and flow:

Creating a Safer Internet: Key Recommendations

To create a safer and more responsible internet for everyone, it’s essential to recognize the challenges we face and take action. Based on my research, I propose the following solutions:

1. **Acknowledge the Problem:** The first step is to realize the issues we face in cyberspace, particularly concerning cybercrime and online safety.
2. **Enforce Cybercrime Laws:** It is necessary to establish laws specifically targeting cybercrime to ensure better regulation and accountability.
3. **Establish a Dedicated Ministry:** A separate ministry should be created to oversee cybercrime laws and policies.
4. **Independent Enforcement Body:** A new, independent body should be formed to enforce these laws. This body should have powers similar to law enforcement agencies, such as the police.
5. **Appoint IT Experts:** The enforcement body should include well-educated scholars and professionals from the IT sector to ensure effective implementation of the laws.
6. **Create a Cyber-Forensics Lab:** A dedicated lab should be set up to investigate cybercrimes and analyze digital evidence.
7. **Build a Cyber-Data Repository:** Establishing a secure cyber-storehouse will help manage digital evidence and information related to cybercrime.
8. **Internet Access Regulation:** To prevent misuse, we should create a system where individuals can only access the internet by providing their National ID or Birth Certificate number.
9. **Promote Internet-Based Education:** It is essential to provide education on internet safety and cybersecurity through online platforms to reach a wider audience.
10. **Raise Public Awareness:** Public awareness campaigns are crucial to ensure that people understand the importance of cybersecurity and comply with the law.

By implementing these recommendations, we can create a safer, more secure internet environment for all.

This version makes the recommendations clearer and more concise while maintaining the essence of your ideas.

6.5 Conclusion:

In the evening, it’s important to highlight that without proper education about the internet, we cannot create a safe online environment. To build a digital country, strong laws need to be established based on current situations. By following these recommendations, we can find effective solutions. It’s also crucial to consider that all cybercrimes should be treated like civil crimes. Immediate action is needed to protect our country.

BIBLIOGRAPHY

Books

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

List of Statutes

1. The Information and Communication Technology Act, 2006
2. Digital Security Act 2016
3. The Penal Code, 1860 (Act No. XLV of 1860)2.
4. Bangladesh Telecommunication Act 2001
5. Criminal Code of Procedure 1898
6. Pornography Act 2012
7. The National Information and Communication Technology (ICT) Policy (October, 2002).

Journals

1. Duggal Mr. Pavan,'Causes of Cyber', Intenational Journal of Computer Science and Information Security, Vol.3, No. 1(October, 2009).
2. Biswas Ripon Kumar, 'Cybercrimes need more attention,' Tuesday, September 09, 2008

Websites

1. <[http://www.naavi.org/pati/pati_cybercrimes_dec03.htm>
2. <Daily ProthomAlo (12 March, 2012),[http://www.bangladeshnews24.com/prothomalo/newspaper/ >
3. <http://www.slideshare.net/fakrulalam/bangladesh-cyber-security-status-in-global-perspective>
4. < http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>
5. <http://www.mid-day.com/articles/cyber-crime-doubles-in-navi-mumbai-in-2-years/15989157.>
6. <http://tech.firstpost.com/news-analysis/5-things-all-broadband-users-must-know-81724.html >
7. <http://wirelessbangladesh.blogspot.com/2009/04/internet-history-of-bangladesh.html?m=1>
8. <httpwww.bdlawdigest.orgcyber-crime-a-new-menace-in-modern-era>
9. <http://www.risingbd.com/english/cyber-crime-in-bangladesh-a-growing-threat-in-digital-marketplace/28940>
10. <http//www.progressbangladesh.com/maximum-14-tears-in-jail-for-cyber-crimes/>
11. <http://www.banglajol.info/index.php/NUJL/article/viewFile/18529/12979>
12. <https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx>
13. <http://sufi-faruq.com/en/combating-cybercrime-a-bangladeshi-perspective-2/>