

Cybercrime and its impacts: A review
(Critically analyzing the impacts on Bangladesh and possible solution)



Submitted by

Zenith Alom Keka

ID: 212-38-431

Submitted to

Mr. Arif Mahmud

Lecturer(Senior Scale)

Department of Law

Daffodil International University

Date of Submission: 12 January, 2022

LETTER OF APPROVAL

10 January, 2022

Arif Mahmud

Department of Law

Daffodil International University

Subject: Cybercrime and it's impacts: A review

Dear Sir,

It is a great pleasure for me to submit a paper on cybercrime and its impact : A review , critically analyze the impacts on Bangladesh and its solution . During preparing this research paper I did my dimension best to keep up the required standard.

I , hereby do solemnly declare that this work has done by me and there is nothing copyright.

I believe that this research paper will satisfy your desire.

Zenith Alom Keka

.....
Zenith Alom Keka

ID: 212-38-431

LL.M.

Mobile: 01761986295

Email: zenith26-1105@diu.edu.bd

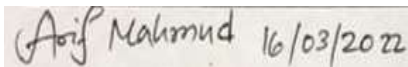
Department of Law

Daffodil International University

DECLARATION

I am Zenith Alom Keka, ID: 212-38-431, student LLM in Daffodil International University here by declared that this research on the topic “Cybercrime and its impacts: A review” has been conducted by me and I am ensuring that this is my own work. There is nothing copied in it, this work is completely unique and has never been submitted before.

This work has been conducted for LL.M thesis.



.....

Zenith Alom Keka

ID: 212-38-431

Department of Law

Daffodil International University

ACKNOWLEDGEMENT

At the beginning of my paper I would like to thank some peoples who inspired me a lot to prepare the paper.

First of all, I would like to thank Almighty Allah for giving me ability, knowledge, capacity to work with patience and opportunities. I am thankful to my supervisor for supporting and guild me such an effective way without his support it was not possible for me to complete the work. Lastly, I would like to thanks my beloved family who always support and encourage me mentally and financially without their support it was impossible to stand here.

DEDICATION

I would like to dedicated my work to my beloved family who always support and encourage me mentally and financially without their support it was impossible for me to stand here.

ABSTRACT

In the current era of online processing, most information is online and prone to cyber threats. There are a lot of cyber threats and their behavior is difficult to understand in the beginning so it is difficult to limit the initial stage of cyber attack. There may be some motive behind the cyber attack or it may have been processed unknowingly. The attacks that are deliberately carried out can be considered as cyber crimes and they have a serious impact on the society in the form of economic catastrophe, mental disorder, threat to national defense etc. The limitations of cybercrime depend on an accurate analysis and understanding of their behavior. Their impact on different levels of society. Therefore, the current manuscript provides an understanding of cybercrime and its impact on society with future trends in cybercrime.

Table of Content

Letter of Transmittal.....	i
Letter of Approval.....	ii
Declaration.....	iii
Acknowledgement.....	iv
Dedication.....	v
Abstract.....	vi

Chapter-1

Introduction

1.1. Introduction.....	1
1.2. Background of the study.....	1
1.3. Research Questions.....	2
1.4. Methology of the study.....	2
1.5. Literature review	2-3
1.6. Significance of the study.....	3
1.7. Objective of the study.....	3
1.8. Concept of the study.....	3

Chapter-2

2.1. Definition of cybercrime.....	4
2.2. Types of cybercrime.....	4-5
2.3. Tools of cybercrime.....	5

Chapter-3

3.1. Effects.....	6-7
3.2. Present situation in Bangladesh.....	7-9
3.3. Prevention.....	9

Chapter-4

4.1. Existing Laws of cybercrime in Bangladesh.....	10-11
4.2. Loopholes.....	11

Chapter-5

5.1. Cybercrime in different countries	12
5.2. Recommendation.....	13-14
6. Conclusion.....	15
7. Refferences.....	16

Chapter 1

Cybercrime and its impacts: A Review (Critically analysis the impacts and solution)

1.1. Introduction

In the modern day, it is quite simple to leverage the time element to boost performance. This is only feasible when we connect to the internet. The term "Internet" refers to a network of millions of computers that act as a hub for electronic communication between computers. While everyone recognizes the benefits of the Internet, cybercrime has a dark side that has a major influence on society in the form of economic conflicts, mental problems, and dangers to national defense, among other things. Internet space, or cyberspace, is expanding at a breakneck pace, as is cybercrime.

The following are some of the several types of cyber criminals:

- **Crackers:** They want to cause harm in order to further some antisocial goals or simply for the sake of having fun. Numerous creators and distributors of computer viruses fall into this category.
- **Hackers:** They may be attempting to acquire access to more powerful computers, earn the respect of fellow hackers, establish a reputation, or win acknowledgment as an expert without obtaining official schooling.
- **Prankstars:** They plan on others but are not interested on causing significant or long-lasting harm.
- **Criminals as a career:** They derive a portion or all of their money from crime. They are not often associated with crime as a full-time vocation for the mentally ill. Someone has a job, earns a little money, and then moves on to another job.
- **Cyber terrorists:** Cyber terrorists come in a variety of forms. Occasionally, a clever hacker will gain access to a government website, and occasionally, a group of like-minded Internet users will crash a website by overwhelming it with traffic.
- **Cyber bulls:** Cyberbullying is a form of online harassment.

1.2. Background of the study

Computer crime is an act done by an inexperienced computer user, commonly referred to as a hacker, who illegally browses or steals another person's information. This individual or group of individuals may occasionally cause damage to or corruption of the computer or data files. Debarati Halder and K Jaishankar define cybercrime from a gender perspective, describing it as "crimes perpetrated against women with the objective of hurting them psychologically or physically through the use of the internet and mobile phones." Occasionally, the term "cyber warfare" is used to refer to action that transcends international borders and involves at least one nation state. The annual cost to the global economy, according to a report sponsored by McAfee, is projected to be \$445 billion. According to Juniper Research, cybercrime might cost up to 2.1 trillion dollars by 2019.

1.3. Research Questions

- What is cybercrime and what are its subtypes?
- What tools are employed in cybercrime?
- What are the impacts of increasing cybercrime in Bangladesh ?
- How to control cybercrime in Bangladesh and what are the loopholes?
- How to control cybercrime in another countries?
- What can be solution to control cybercrime properly ?

1.4. Methodology of the study

The research focused at analyzing the current scenario of cybercrime in Bangladesh and its impacts on Bangladesh and this research also give the jurisdiction and some recommendations for solving this issue. With the view of addressing the question , a thorough study will be conducted by considering the definition of cybercrime, types, tools, impacts, present scenario in Bangladesh , cyber laws etc.

For the purpose of collecting the relevant material for the research , I studied the international data , Wikipedia of cybercrime , various pdf files and various research papers and various acts(ict act .

Now I want to add among those research- how Bangladesh facing the problems during increasing the crime rete , what are the loopholes and recommendations.

From my view it is the serious issue that how we solve the crisis and for solving this crime there are some recommendation are given in the research paper.

1.5. Literature review

Computer Crime is an act performed by a knowledgeable computer user , sometimes reffered as a hacker that illegally browses or steals an individual's information . In some cases , this person or group of individuals may be destroy or otherwise corrupt the computer or data files. The cyber crime included cyber squatting , cybersex , child pornography , identity theft , illegal access to data . Internet is the backbone of all kinds of communication system and it is one of the most important sources of the knowledge in the present era .It is consisted of millions of public and private , academic business and government networks of local to global scope that are linked by copper wires ,fiber cables , wereless connections and other technologies.Presently Bangladesh has already become a victim of cyber crime . The incident of Bangladesh Bank heist is one of the proven evidences . Legal response to cyber crime in Bangladesh in order to facilate e-commerce and encourage the growth of information technology . The Information and Communication Technology Act , 2006 was enacted where the maximum punishments are 10 years imprisonment or fine upto taka 10 million or both . However the National Parliament amended the ICT Act 2006 . The cabinet approved the draft of the ICT Act 2013 on August 19 proposing to empower law enforcers to arrest any

person without warrant and increase the highest punishment to 14 years from minimum 7 years or a fine taka 1 core or both . The bill made offences under sections 54 , 56 , 57 and 61 of the ICT Act 2006 cognizable and non – bailable . However all concerned apprehend of the misuse of the power by the police . The ICT Act , 2006 as amended in 2013 is obviously a brilliant achievement of Bangladesh in the field of cyber law .

1.6. Significance of the study

Nowadays cybercrime is the alarming issue and everyone has interested and has their own opinion on it.

Presently Bangladesh has already become a victim of cybercrime.

The research is focused on present condition of cybercrime on Bangladesh , the cyber law .I think the research is significance to know about the cybercrime and for analyzing causes and the solution of cybercrime .

So, this research is significant for understanding the impacts and solutions of cybercrime in Bangladesh.

1.7. Objective of the study

The main object of the research is to understand the causes and impacts of cybercrime in Bangladesh .

The objectives of the research paper are given below:

- To know about the definition of cybercrime , types and tools.
- To know about the impacts of cybercrime in Bangladesh and other countries.
- To know about the cyber laws in Bangladesh and how to control cybercrime in Bangladesh and other countries.

1.8. Conceptual Understanding

The concept is for or understanding the cybercrime and its impact on Bangladesh and also the concept is additionally knowing and identifying the cyber law in Bangladesh.

Chapter 2

2.1. Definition

Cybercrime is a type of crime that involves the use of a computer and a network. Occasionally, the computer is used to commit a crime or is the target. It could jeopardize someone's security and financial well-being. It has a significant impact on society in the form of economic conflict, psychological dysfunction, and a threat to national defense, among other things. Cybercrime is done by cybercriminals or hackers for financial gain. Individuals or groups carry it out. Cybercrime's objective is to cause damage to computers for non-monetary gain. This may be political or personal in nature.

According to the United States Department of Justice, cybercrime is broken down into three types:

Computer-related crimes include those in which the computing device is the target—for example, obtaining network access—and those in which the computer is used as a weapon, such as launching a denial-of-service (DoS) attack. Additionally, it stated that crimes involving the use of a computer as an accessory to a crime are prohibited—for instance, using a computer to store unlawfully obtained data.

The Council of Europe Convention on Cybercrime defines cybercrime as a wide range of hostile acts, including illicit data interception, system interferences that jeopardize network integrity and availability, and copyright infringements.

2.2. Types

The Internet may be a frightening world filled with scammers, thieves, and saboteurs. According to the Norton Cyber Security Insights Report, over 143 million Americans have been impacted by computer crimes in the last year, with 80 percent of those polled stating that they or someone they knew had been a victim. From theft to fraud to solicitation, here are five of the most prevalent Internet crimes affecting the entire world.

- 1) **Hacking:** Hacking is a type of crime in which a person's computer is hacked in order to gain access to his personal or sensitive information. It is considered as a criminal offense in the United States. In hacking, the criminal employs a variety of tools to gain access to a victim's computer, which the victim may be unaware of.
- 2) **Theft:** Theft occurs when someone breaks copyright laws and downloads music, movies, games, and software. At the moment, the justice system is combating cybercrime, and there are rules against unauthorized downloading.

- 3) **Cyberstalking:** Cyber stalking is a form of online harassment in which the victim is bombarded with online messages and emails. The stalker stalks over the internet. If they see that internet stalking is having the desired impact, they switch to offline stalking in order to make the victim's life unbearable.
- 4) **Identity theft:** Identity theft has become a significant issue as more individuals use the internet for financial transactions and banking services. In this crime, a criminal obtains access to a victim's bank account, credit cards, social security number, and other identifying information in order to make online purchases in the victim's name. It has the potential to result in significant financial losses for the victims.
- 5) **Child Abuse:** Child Abuse is also a type of cybercrime in which criminals utilize chat rooms to lure youngsters for the purpose of child pornography. The FBI has spent considerable time monitoring chat rooms popular by youngsters in an effort to curb child abuse.

2.3. Tools

There are numerous sorts of digital forensic tools, including the following:

- **Kali Linux:** Kali Linux is an open-source operating system that is developed and maintained by Offensive Security. It is an application that has been built for digital forensics and penetration testing.
- **Ophcrack:** It is mostly used for cracking hashes created by the same Windows files. This utility features a secure graphical user interface and is cross-platform compatible.
- **EnCase:** EnCase is a type of software application. It enables investigators to scan and study data stored on hard disks and removable storage devices.
- **SafeBack:** SafeBack is primarily used to image the hard drives of Intel-based computer systems and to restore these images to another hard disk.
- **Data dumper:** It is a command-line-based computer forensics program. This is a free program for the UNIX operating system that allows for accurate disk copies appropriate for digital forensic examination.
- **Md5sum:** A check tool assists you in determining whether data has been successfully copied to another storage location.

Chapter 3

3.1. Effects

1. Consequences of Cyber Crime

A cyber attack can have far-reaching consequences, including as financial losses, intellectual property theft, and a loss of consumer confidence and trust. Every year, the economic impact of cybercrime on society and government is estimated to be in the billions of dollars. Criminals take advantage of technology in a number of ways. The Internet, in particular, is a wonderful tool for fraudsters and other miscreants since it allows them to do their business while remaining anonymous online. Cybercrime has many negative consequences for society, including the following:

- **Identity Theft:** Cybercrime can have a long-lasting impact on a victim's life. Scammers use a general technique called phishing, in which they send phony emails purporting to be from a bank or other financial institution asking personal information. If someone provides this information, the offender gains access to his bank and credit accounts, as well as the ability to open new accounts and damage his credit rating.
- **Security costs:** Cybercriminals attack businesses of all sizes. Hackers may try to obtain access to a company's servers in order to steal data or utilize computers for personal advantage. According to E-week, large corporations spend an average of \$8.9 million per year on cybersecurity, with 100% of businesses reporting at least one malware incident in the preceding year and 71% reporting computer hacking. by complete strangers.
- **Monetary loses:** The financial costs of cybercrime can be enormous. According to a 2012 Symantec analysis, more than 1.5 million people are exposed to cybercrime on a daily basis, ranging from basic password theft to enormous financial fraud. With an average loss of \$197 per victim, this equates to a global loss of more than \$110 billion in cybercrime each year. As customers become more sophisticated in their traditional attack methods, cybercriminals have developed and used new approaches to integrate mobile devices and social media in order to maintain their illicit gains.
- **Piracy:** Piracy, a form of cybercrime, has had a significant impact on the entertainment, music, and software sectors. Copyright holders have advocated for stronger intellectual property theft regulations, which have resulted in legislation such as the Digital Millennium Copyright Act. These rules enable copyright holders to pursue file sharers and sue them for substantial sums of money in order to compensate for the financial harm caused by their online activities.

2. **Social Impacts :** Because thieves exploit anonymity, privacy, and interconnectedness on the Internet, our modern information attacks the very pillars of society. Botnets, cyber terrorism, computer viruses, cyber bullying, cyber stalking, cyber pornography, distributed denial of service attacks; hacktivism, identity theft, malware, and spam are all examples of cybercrime. Law enforcement agencies have battled to keep up with cybercriminals, who wreak havoc on the global economy on a yearly basis. The technologies that cybercriminals use to conduct crimes are also employed by law enforcement to prevent such crimes and prosecute those responsible. It begins by defining cybercrime and then discusses its economic and social consequences. It then delves into cyber bullying and cyber pornography, two particularly egregious forms of cybercrime, before concluding with a discussion on strategies to combat cybercrime's spread. Cybercrime dates all the way back to the dawn of computing, despite the fact that the increased connectivity of computers via the Internet has pushed information into the general consciousness of society. "Already, billions of dollars' worth of losses have been discovered. Additional billions could not be identified. Trillions of dollars could be taken by the rising primary perpetrator of twenty-first-century online criminals, most of whom operate anonymously."
3. **Emotional Impacts of Cyber Crime :** A new report from Norton finds an astounding surge in cybercrime, with about 65 percent of Internet users globally and 73 percent of US web surfers becoming victims of cybercrime, which includes computer viruses, online credit card fraud, and identity theft. The United States ranks third in terms of impact, behind China (83 percent), Brazil, and India (76 percent). Psychological research on the psychological effects of cybercrime demonstrates that victims are most likely to feel angry, upset, and deceived, and frequently blame themselves for the attack. Only 3% believe it will not happen to them, and approximately 80% believe cybercriminals will not be prosecuted, resulting in an absurd reluctance to act and feelings of helplessness. Despite the psychological toll, public threats, and cybercrime, people's behaviors remain unchanged - 51% of adults say they would alter their conduct if they were a victim. Even fewer than half (44%) reported the crime to the authorities. Around 80% of cybercrime is believed to be the result of organized crime. The proliferation of fraudulent models as a service and the breadth of underground market offerings are also attracting new actors with only rudimentary skills. Cybercrime is a lucrative economic opportunity available to anyone who is motivated by profit and personal gain.

3.2. Present scenario in Bangladesh

1) Bangladesh is a developing country, according to the United Nations. Access to information is limited in most poor nations, including Bangladesh, due to a lack of understanding about existing infrastructure. Cybercrime is a theft of property. Victims are not prioritized here; the crime's sole objective is to grab property like as information, data, and so on. The majority of banks in Bangladesh face significant security risks. According to the Bangladesh Institute of Bank Management (BIBM), the banking and information technology sectors received approximately Tk 1,693 crore in investment in 2017. However, our country's banking industry is not immune to cybercrime. According to a survey conducted by the Bangladesh Institute of Bank Management (BIBM), 52% of our country's banks face a high

risk of cyber security breaches. Among these 52% of banks, 16% are extremely high risk and 36% are high risk. Some (32% of banks) are considered medium risk, while others (12%) are considered to be low risk, and 4% of banks are considered to be extremely low risk. Cyber security in the banking sector is a hot topic now, especially in the aftermath of the Bangladesh Bank robbery. The Bangladesh Bank's history began on 4 February 2016, when hackers (who remain unidentified) attempted to steal \$1 billion. The hackers sent 81 million in four different transfer requests to the Philippines' Rizal Commercial Banking Corporation and Sri Lanka's PABC Bank, as well as another 20 million in a request to Pan Asia Banking. Evtldiag.exe was the malware's filename. Reuters was the name of the assailants. The hacker accomplished this via malware. Before they are dispatched to the workplace printer, this spyware deletes incoming messages and confirmation messages. The malware became active on February 4 after business hours. Due to the fact that Friday was a holiday in Bangladesh, there was no one to supervise the crossing. The assailant made many relocation petitions, but all were denied. They continue to attempt transfers until they are able to deposit funds into their fictitious account. Then, when the bank reopened on Sunday following the weekend, officials discovered something was amiss since the malware had also prevented the printer from printing the conversion information. Malware controls login and logout operations, as well as servers and configuration updates. They subsequently requested that the Philippine Bank halt transit, but the weekend was approaching in the Philippines. The infection was set to run until February 6. The transfer was halted after the attempt was discovered, yet the attacker was still able to move \$ 81 million.

2) A report by the Cyber Crime Awareness Foundation indicates that social media account hacking has increased from 13% in 2019 to 28% in 2021. According to the report, social media and other online accounts are now hacked at a rate of 28.31 percent. According to the age-based analysis of cybercrime, the majority of victims are between the ages of 18-30, accounting for 8.90 percent of all victims.

3)

- According to a recent survey, more than 70% of kids encounter online cyberstalking, bullying, or blackmail, with around 75% reporting that they or their seniors have been sent or asked to share clear messages, photos, or videos.
- Only 13.4 percent of victims sought assistance from their parents, while 15.9 percent sought assistance from their professors. Only 7%–35% indicate a willingness to seek assistance from law enforcement, the police cybercrime section, or specific applications, helplines, or websites.
- A sizable portion of Internet users are likely teenagers who gained access to the Internet for academic purposes as a result of schools and colleges being closed during the epidemic.
- Last year, police headquarters established a helpline for women dealing with cybercrime via emails, Facebook pages, and a toll-free hotline.

- According to Cyber Support for Women data, 12,641 complaints related fake IDs, ID hacking, extortion, and obscene content were filed between November 2020 and October 2021.

4) Until this year, there was only one cybercrime tribunal in Dhaka, Bangladesh. According to records, the tribunal received 33 cases in 2014 and subsequently climbed to 1,189 in 2019. In 2020, 1,128 cases were reported, and by March 2021, there were 447.

3.3. Prevention

It is natural to conclude that almost no one is immune to victimization. However, the prevalence of cybercrime does not imply that victimization is a foregone conclusion or that individuals should abstain from using the Internet. Users can be aware of the risks associated with its use and take actions to mitigate them.

- Use strong password: Use unique ID/Password combinations for each account and avoid writing them down. By mixing letters, numbers, and special characters, you can create complex passwords.
- To safeguard your computer: Firewalls are the first line of protection against cyber attacks; they filter out questionable traffic and keep out specific sorts of viruses and hackers.
- Use Anti virus or malware software: Anti-virus/malware software should be installed and updated on a regular basis to prevent viruses from invading your computer.
- Protect your mobile device: Keep in mind that mobile devices are susceptible to viruses and hackers. Download apps only from reputable sources. Keep no superfluous or sensitive data on your mobile device.
- Update your operating system: Maintain up-to-date applications and operating systems, such as Windows, Mac, and Linux, with the latest system updates. Enable automatic upgrades to safeguard against potential attacks on outdated software.
- Safeguard your data: Encrypt all sensitive files, including medical records, tax filings, and financial records. Backup all critical data on a regular basis.
- Secure the wireless network: If not adequately secured, Wi-Fi networks are susceptible to penetration. Conduct a review and modification of the default settings.
- Avoid being scammed: Avoid becoming a victim of fraud by refusing to respond to emails requesting verification of your personal information or confirmation of your user ID or password. Avoid clicking on links or downloading anything from unknown sources. If in doubt, verify the source, the message's source.

Chapter 4

4.1. Existing Laws of cybercrime in Bangladesh

1) Article 43 of the 1972 Bangladesh Constitution protects people' correspondence and communication privacy.

According to Article43, every citizen has the right to reasonable restrictions imposed by law in the interest of state security, public order, public morality, or public health in order to secure his home against unauthorized entry, search, or seizure; and to the privacy of his correspondence and other means of communication.

2)In accordance with Section 63 of the ICT Act, 2006, the penalty for disclosing a confidential or private electronic record, book, register, communication, information, document, or other material without the consent of the person involved is a fine of up to ten thousand dollars. The penalty for such unauthorized disclosure of such records may be up to two years in prison or a fine of up to Taka two lakhs.

3)The Digital Security Act,2018, as a cyber security law, seeks to promote confidentiality and integrity with the objective of safeguarding individual rights and privacy, commercial interests, and data protection in the internet.

4) Section 26 of the Digital Security Act defines personal data as "identification information" that must be collected, sold, preserved, supplied, or used with the consent or authorization of the individual. Under this article, any infringement is punishable by five years in jail or a fine of Taka 5 lakhs, and the penalty escalates to seven years in prison or a fine of Taka 10 lakhs in the event of a subsequent offense.

5) Section 34 of the Digital Security Act makes hacking a serious offense punishable by up to 14 years in prison or a fine of up to Taka 1 crore, or both.

6) Section 71 of the Telecommunications Act, 2001 imposes a six-month prison sentence or a fine of Taka 50,000 on those who eavesdrop on telephone conversations.

7) However, a 2006 change to the legislation exempts police enforcement agencies from prosecution under section 97A on the grounds of state security or public order.

8) The Penal Code 1860 penalizes the infringement of privacy by criminal breach of trust under sections 407,408, and 409. According to Section 407, anyone who is entrusted with property as a professional or warehouse-keeper and commits a criminal breach of trust in such property is subject to imprisonment of either sort for a period not to exceed seven years, as well as a fine. According to Section 408, Anyone who is a clerk or servant, or who is employed as a clerk or servant, and is entrusted with property or has dominion over property in any capacity, Commits criminal breach of trust in relation to that property, and is punished by imprisonment of either kind for a term not exceeding seven years, as well as a fine. According to section 409, Anyone who is entrusted with property or has dominion over property in his capacity as a public servant

or in the course of his business as a banker, merchant, factor, broker, attorney, or agent commits criminal breach of trust in relation to that property is punishable by life imprisonment or a term of imprisonment of either description not exceeding ten years, as well as a fine.

9) Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR), to which Bangladesh is a party, states that no one shall be subjected to arbitrary or unlawful interference with his or her private, family, home, or correspondence.

4.2. Loopholes

This act has some specific limitations. They are :

- (a) The law is silent on various intellectual property rights such as copyright, trademark and patent rights to e-information and data.
- (b) The law has had a significant impact on Bangladesh's e-commerce sector. But it also keeps the electronic payment of any transaction.
- (c) Originally, the law was intended to apply to crimes committed anywhere in the world; however, no one knows how to accomplish this.
- (d) Spamming has become a threat in the Western world as a result of anti-spamming laws incorporated into cyber law. However, our law contains no anti-spam provisions.
- (e) Domain names are a significant issue that are inextricably linked to the Internet world.
- (f) This act makes no reference to criminal activity involving the use of mobile phones.
- (g) The law makes emails admissible as evidence, contrary to the country's evidence law, which does not recognize e-mails as admissible evidence.

The Cyber Tribunal shall be presided over by a Sessions Judge or an Additional Sessions Judge and shall consist of a three-member bench, including a Chairman who is qualified to be a former or acting Judge or a Supreme Court Judge, a former or acting District Judge, and one. The cyber appeal tribunal will be presided over by the ICT specialist and two other members of the bench. The public prosecutors will bring a case on the state's behalf in this matter. The issue is that judges and lawyers are specialists in law, not technology. As a result, judges and attorneys must be qualified and knowledgeable about technological issues in order to provide justice in technical disputes.

Chapter 5

5.1. Cybercrime on different countries

- 1) **United State Of America:** According to the Norton Cyber Security Insights report, cybercrime affected over 143 million Americans in 2017, and cybercrime is on the rise in the US. Around 8 to 10 percent of US consumers questioned claimed being a victim or knowing someone who was, so it's understandable that Americans are more concerned about cybercrime than other types of crime. To protect the interests of Internet businesses in the United States, the US Congress has enacted new laws regulating Internet activity. The US Congress has implemented a variety of regulations addressing cybercrime, such as the "National Infrastructure Protection Act of 1996" and the "Cyberspace Electronic Security Act of 1999". Additionally, the FBI, the National White Collar Crime Center, computer hacking, and intellectual property divisions have been established in the United States to tackle cybercrime.
- 2) **England :** England's Parliament has enacted two cybercrime legislation, the 1984 Data Protection Act and the 1990 Computer Abuse Act. The former is concerned with the actual gathering and use of personal data, whereas the latter is concerned with the establishment of laws, procedures, and sanctions. Surrounding illegal computer access. To protect manors from inappropriate web content, the British government has implemented filtering and rating technology.
- 3) **Canada:** In 2001, the Canadian Parliament passed the Criminal Law Amendment Act, which has two provisions. The first section describes unauthorized access to a computer system and a transmission barrier. The second category criminalizes the act of actually destroying, altering, or obstructing data.
- 4) **India:** According to data from the National Crime Records Bureau, India reported 50,035 cybercrime cases in 2020. Continue reading to learn about the motivations behind approximately two out of every three similar crimes. Additionally, the NCRB gives information about the motivation for the cybercrime that was committed and registered. Fraud has emerged as the primary 'motive' in 30,142 or 60% of all cybercrime detected in 2020. This was followed by sexual exploitation (3,293 cases, or approximately 8% of all cases), extortion (2,440 incidents), disrespect (1,706 cases), and personal retribution (1,706 cases) (1,460 cases). In 2020, these five motives will account for 78 percent of all cybercrime recorded.
- 5) **Germany :** According to the Federal Office of Information Security's (BSI) IT Security Situation Report 2021, the degree of threat to IT security in Germany is higher than ever before, owing to an increase in cyber threats and the emergence of more professional cyber criminals. The report demonstrates a tremendous increase in cybercriminal extortion techniques known as ransomware assaults, as well as a dramatic increase in new forms of malware, software designed to obtain access to interrupted, damaged, or unauthorized computer systems.

5.2. Recommendation

Cybercrime is finally receiving the attention it so richly deserves. However, it will not be simply contained. Indeed, cybercrime and its hackers are likely to evolve and improve in order to remain one step ahead of the law. As a result, cyber security is necessary to keep us safe. While there is little doubt that technical defenses are superior to legal remedies in terms of avoiding high-tech crime, such defenses are susceptible to being destroyed because they are not permanent. Those with more advanced technology than we have the ability to breach the security wall at any time. As a result, legal and other recourses are required to address the aforementioned situation. Along with existing remedies, the state may pursue some new initiatives similar to those pursued by some of the world's most advanced high-tech states. Consider the following characteristics:

- I) Bangladesh is a constitutional monarchy. The Constitution is critical in preserving and ensuring both the people's and state's rights and obligations. The constitutional provision against cybercrime has the potential to elevate cyber warfare to a national level, which is a superior form of organization to any other. Additionally, there are legal remedies. Constitutional amendments could be used to enact such provisions.
- II) Special Wing of Police: To ensure a peaceful cyber cloud in a digital Bangladesh, we must provide law enforcement authorities with training and technology. Cybercriminals are not the adversaries of any particular country or region; they are the world's common enemy. The residents of the twenty-first century must band together to defeat their adversaries. The development of cybercrime has compelled law enforcement to operate on a worldwide scale rather than as a regional or national one. The police force must be equipped to address the difficulties of technology in combating all crimes, including cybercrime, through global cooperation. The United Kingdom, the United States of America, India, and Malaysia, among other developed countries, have established special sections of law enforcement to combat cyber warfare. Bangladesh may establish such a specialized police wing in addition to other preventive steps against high-tech dangers.
- III) Cyber Crime Agency by Government: North Korea twisted the Korea Internet and Security Agency²⁵, a government agency formed by the merger of North Korea's previous three Internet technology companies, on July 23, 2009. Now, the agency will work to transform North Korea into a developed, strong, and secure country in terms of internet access. Several other countries, including India, have established similar institutions. Given Bangladesh's current state of internet usage and cybercrime, the government may also establish such an institution. The value of such agencies is that they will be capable of performing a variety of functions, including improving Internet infrastructure, maintaining ISPs, regulating Internet usage charges, and preventing cyber threats.
- IV) Watch Dog Group: This group is primarily concerned with Internet-based security intelligence. These tasks include collecting and analyzing dangerous software, isolating and analyzing sandboxing and viruses and trojans, monitoring and reporting malicious attackers, and spreading cyber-threat information. The notion of this dog is not new. The Shadow Server Foundation, created in 2004, is an example of a watchdog organization. These can be both private and public. There

is no such organization in Bangladesh at the moment, but given the growing cyber threat, these dog groups could play a significant role in transforming Bangladesh into a developed country, particularly in terms of internet technology.

- V) Public Awareness: This training is just as critical as a technological preventative step, as the majority of the time, ordinary people are exposed to cyber attacks, resulting in the destruction of millions of computers. Therefore, if it is possible to educate people about the nature, potential barriers, and antidote to threats, it will be easier to defeat cyber criminals and save the virtual world, and the government can play a significant role in this effort. As with other critical issues, the government should raise public awareness through various media outlets. Additionally, non-governmental organizations and other groups can launch a campaign in this direction.

Chapter 6

Conclusion

Cybercrime is growing at a rapid pace, but our government is attempting to defend it. Every citizen should be informed of this. It is becoming a huge menace to people around the planet. It is crucial in today's society to create awareness about how information is being protected and the strategies that thieves employ to acquire that information. There are 1.5 million cyber attacks per year, which equates to over 4000 per day, 170 per hour, or about three per minute. According to the poll, just 16% of victims who committed the attack were instructed to cease. Anyone who uses the internet for whatever purpose is at risk of becoming a victim, which is why it is critical to understand how one is protected online.

References

There are no sources in the current document.

- 1) Mathews.B.(2008)computer crimes : cybercrime information , Facts and resources , available at <http://www.thefreeresource.com/computer-crimes-cyber> information (accessed on 7 June2015)
- 2) International Journalof Engineering sciences and emerging Technologies ,'vol.6, no.2, 2013 , pp. 142-153 available at [http://www.privacyrights.org/content/childrens-safetyinternet\(accessdon](http://www.privacyrights.org/content/childrens-safetyinternet(accessdon) 1 July2017)
- 3) The office of Angel Cruz , chief information security officer , state of taxes September 2012, volume6, issue 8.
- 4) Cybercrime [Definition , statistics and examples] Britannica” <http://www.britannica.com> . Retrived 14 December 2021
- 5) Bangladesh Bank Attackers Used Custom Malware,” <https://www.pcworld.com/article/3060724/> bangladesh-bank-attackers-used-custom-malware.
- 6) “Bangladesh bank heist, swift software was compromised,” [https://www.itgovernance.co.uk/blog/](https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2017/) list-of-data-breaches-and-cyber-attacks-in-april-2017/
- 7) “Ict ministry news,” [http://doict.portal.gov.bd/site/page/](http://doict.portal.gov.bd/site/page/73fa42ac-fae9-4c0b-bec7-5edbb6841e64/) 73fa42ac-fae9-4c0b-bec7-5edbb6841e64/.
- 8) “Dhaka tribune news,” <http://www.dhakatribune.com/business/banks/2017/05/05/banks-high-cyber-risks/>.
- 9) “Bangladesh bank heist, swift software was compromised,” [http://www.reuters.com/article/](http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR) us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR.
- 10) “Cyber crime scenario in bangladesh,” [http://www.icmab.org.bd/](http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf) images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf.
- 11) “Ict amendment 2013,” [http://www.askbd.org/ask/2013/10/09/](http://www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat/) ict-amendment-act-2013-information-freedom-expression-threat/.
- 12) “Ict act 2006,” [http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/97cc59c3_8f51_4d39_a84b_8c0b39ae3f62/](http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/97cc59c3_8f51_4d39_a84b_8c0b39ae3f62/ICT_ACT_2006.pdf) ICT_ACT_2006.pdf.
- 13) “Ict act 2006 bangladesh,” http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=950&vol=37&search=2006/, [Online; accessed 25-September-2017].
- 14) “Ict act 2009 bangladesh,” http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=1011&vol=39&search=2009/, [Online; accessed 25-September-2017]
- 15).Moore , R . (2005) “Cyber crime : Investing High Technology Computer Crime ,” Cleveland , Mississipi : Anderson Publishing .
- 16) Steve Morgan (January 17 , 2016) “ Cyber Crime Costs Projected To Reach \$ 2 Trillion by 2019 .’ Forbes Retrived September 22,2016 .
- 17) “We talked to the opportunist imitator behind Silk Road 3.0” 2014-11-07 .Retrived 2016-10-04
- 18) “ A walk on the dark side .” The Economist .2007-09-30 .
- 19) Moore,R(2005) “Cybercrime:Investigation High Technology Computer Crime”, Cleveland, Mississipl: Anderson publishing