

**COMBATING CYBER CRIMES IN BANGLADESH: A CRITICAL ANALYSIS IN THE  
CONTEXT OF LEGAL RAMIFICATION OF LAW.**

**Researcher**

Name: M.B. RAQIB

ID: 141-38-241

Program: LLM

Department of Law

Daffodil International University

**Supervisor**

S. M. Saiful Haque

Assistant Professor

Department of Law

Daffodil International University



**Daffodil International University**

**Date of Submission: 11 December, 2018**

# Letter of Transmittal

Date: 11December,2018

S. M. Saiful Haque

Assistant Professor

Department of Law

Daffodil International University

Dear Sir,

After my utmost endeavor I have been able to make a research on “**COMBATING CYBER CRIMES IN BANGLADESH: A CRITICAL ANALYSIS IN THE CONTEXT OF LEGAL**

**RAMIFICATION OF LAW**”. Thereby it’s a great pleasure for us to submit this research paper on the above stated topic. During concluding this research we have made all attempts to make this research useful and up-to-date by gathering all the relevant information in this paper so that it can fulfill one’s thirst for knowledge and your expectation.

Therefore, I will remain grateful to you if you go through this research paper for your evaluation and I would be happy if any valuable suggestion is made from your part in this matter.

I am always available for any clarification of any part of this paper at your convenience.

Thanking you.

Name: M.B. RAQIB ID:

181-38-241

Program: LLM

Department of Law

Daffodil International University.

## **Declaration**

I am **M.B. RAQIB**, ID No: 181-38-241, a student of Law Department of Daffodil International University, hereby declaring that this Research Monograph is the outcome of the investigation and supervision done by me and also prepared by myself under the supervision **S.M.Saiful Haque**, Associate Professor of the Law Department of Daffodil International University.

I also confirm that the paper is only prepared for my academic requirement, not for my other purpose.

**(M.B. RAQIB)**

ID: 181-38-241

Program: LLM (final)

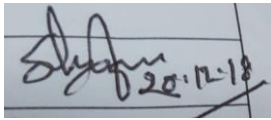
Department of Law

Daffodil International University.

### **Certification**

This is to certify that the work entitled “**COMBATING CYBER CRIMES IN BANGLADESH: A CRITICAL ANALYSIS IN THE CONTEXT OF LEGAL RAMIFICATION OF LAW.**” is an original work by **M.B. RAQIB**, ID No: 181-38-241, Department of Law, Daffodil International University, completed under my supervision and submitted in the partial fulfillment of the requirement for the award of Master of Laws degree,LLM (final), from the Daffodil International University.

I wish him success.



**S. M. Saiful Haque**  
Assistant Professor  
Department of Law  
Daffodil International University

## **Acknowledgments**

I am grateful to Almighty Allah, who has been kind to complete and publish of the research paper successfully. I am grateful to my research supervisor **S.M.Saiful Haque**, Assistant Professor of the Law Department of Daffodil International University who has given proper guidelines to complete my research monograph.

Last but not the least, I express my special thanks to my friend **Muktadir Hasan Rifat** and **Mahfuzul Haq Khan**, to my respected teachers and other professionals for helping and extending their support to me during the research.

Finally, I remember my parents and I offer millions of my heartfelt thanks to Almighty who has given me the strength to complete this research monograph successfully.

**(M.B. RAQIB)**

ID: 181-38-241

Program: LLM (final)

Department of Law

Daffodil International University.

## **Dedication**

I dedicate this research for my parents. Thanks for always being there for me.

## ***Abstract***

*The fear and ignorance of Digitalization is breeding new and dangerous cyber-crimes. The society and academia has a lot of catching up to do in the coming decade. The proper research and legal ramification is of very much importance. Life of innocent and negligent people are being endangered through cyber-crimes. To elucidate and decipher the secrets of illegal activities that obfuscate our civil and social life. The economic effect of the perfunctory digital communication is also a great concern. The quintessential of cyber-crimes is that they are very new and challenging for people who are negligent in their digital interaction. Some sycophants try to use that negligent behavior into their accessory for sinister plans. The legal ramifications against cyber-crimes is next to nothing. New digital media is also serving oppressive authoritative figures to dominate and control the use of free will with surveillance. Overall this research enlarges the focal point of view to include every aspects regarding the cyber-crimes and digital currency. Modern technology have surely eased the human life, and expanded the dimensions of human expectations. And in turn, we have become so much addicted to technology, let it be any field. Technology is a symbol of advancement, but there are side effects of it. We the civilized world needs to strike a balance between the technology and ethics of life, to prolong the impact of the technology on quality life of human beings.*

# Table of Contents

## Chapter-1

### Introduction

1.1 Introduction	1
1.2 Problem statement	1
1.3 Rationale of Study	2
1.4 Research Question	3
1.5 Objective of The study	3
1.6 Literature review	3
1.7 Research Gap	4
1.8 Methodology	4

## Chapter-2

### Classification of cybercrime and recent criteria's

2.1 Hacking	5
2.2 Virus Dissemination	5
2.3 Software Piracy	6
2.4 Pornography	6
2.5 Credit Card Fraud	7
2.6 Sale of Illegal Articles	7
2.7 Online Gambling	7
2.8 Crimes against intellectual property	7
2.9 Email Spoofing 7	2.10 Cyber Defamation 7
2.11 Cyber Stalking	7
2.12 Email Bombing	8
2.13 Data Diddling 8	2.14 Salami Attacks 8
2.15 Reasons to cybercrime	8
2.16 Emerging criteria's and Impact	9

## **Chapter-3**

### **Scenario of Cybercrime in Bangladesh**

3.1 State of Cyber Crime	10
3.2 Impact of Cybercrime against the Government	14
3.4 Cybercrime scenario in Banking Sector of Bangladesh	14
3.5 Case study 1: ATM card skimming.	15
3.6 Case study 2: Bangladesh Bank Heist.	15

## **Chapter-4**

### **Mechanism and Ramifications**

### **Status of Legal**

4.1 National legislative framework	16
4.2 Absence of Specialized Master	17
4.3 Lack of knowledgeable law enforcers	17
4.4 Procedural Difficulties	18
4.5 Lack of Clearance of the Terms	18
4.6 Lack of Sufficient Laws	18
4.7 Civil-Criminals Difficulties	18
4.8 Provincial Systems and the Status of Cyber Law	18
4.9 Global Laws and Traditions on Cyber Law	19
4.10 Other Worldwide Methodologies	19
4.11 Cyber Laws in other Developed countries	20

## **Chapter-5**

### **Cryptocurrencies in Bangladesh**

### **Bitcoins and the Future of**

5.1 Un-traceability and potential threats	20
5.2 Illegality of bitcoins and Law enforcement in Bangladesh	22
5.3 Blockchain mechanism	23
5.4 Legalization by various countries	23

## **Chapter-7**

### **Conclusion**

6.1 Recommendations	25
6.2 Conclusion	26



## ABBREVIATION

ICT.....	Information and communication and technology Act 2006.
DSA.....	Digital security Act 2016.
NDSA.....	National Digital Security Office.
NDSC.....	National Digital Security commission.
EMV .....	Europay, MasterCard and Visa.
BTRC.....	Bangladesh Telecommunication regulatory commission.
BTCL.....	Bangladesh Telecommunication Company limited.
UNCITRAL.....	United Nations Commission on International Trade Law
GATS.....	General Agreement on Trade and Services.
WIPO.....	World Intellectual Property Organization.

## **Chapter –1 - Introductory Discussion**

### **1.1 Introduction:**

In this 21<sup>st</sup> century, we are very much dependent on technology and the world wide web/internet is a most effective and easy source of communication and data resources. As we are digitalizing in every sector day by day and for communication and connecting these sectors as well as regulating and easy access we are getting very much dependent on the web system. As the different sectors are getting dependent on the cyber web, it also raises a question of how safe really the cyberspace is. Along with its easy access and time saving features it has introduced us with some potentially harmful threats such as data diddling, electronic fraud in the financial sector, identity theft, illicit use of valuable information, hacking or cracking, cyber-stalking, distribution of pirated software, terrorism, credit card fraud, spamming, e-money laundering, ATM fraud, Phishing. The most horrified matter is that you don't need any sort of weapon for committing a cyber-offense which is a criminal natured crime itself, all you need is skills, intention, internet connection, and a computer. To regulate such modern crime the most important prevention tool is a modern legislation, which covers every area of cyber-crime issues and which is capable of being interpreted in terms of detecting new threats. There is a sharp rise in the Cybercrimes in Bangladesh and the Law enforcement machinery is finding it really it really difficult to manage these technical crimes in Bangladesh. Cybercrime has already become a going concern in both private as well as the public sector in Bangladesh. During the last decade private and public sector has done a revolution with the use of technical enhancement. Due to unauthorized intervention to the system, the company loses huge confidential information which caused a large amount of financial loss. It has already been identified that especially Financial Institutions are in the most threading organization for cybercrime that at the same time reflects the personal life. Some development partners have started working on how to tackle cybercrime and improve effective communications. In this research, I will be emphasizing How far the Bangladeshi legislation is adequate to minimize and categorize recent emerging forms of cybercrime.

### **1.2 Problem Statement:**

Firstly a cybercrime can be held against an Individual, a property or on an organization or on the society at large. In past few years Bangladesh has seen Bangladesh Bank Heist 2016, skype scandal over International war crime tribunal, Bangladesh computer society website hacked in 2012, Stealing the transaction report of Dhaka stock exchange, Partho threatening prime minister Sheikh Hasina through email in 2004, Inserting porn movies in Bangladesh parliament official website and many more.<sup>1</sup>

In this era of smartphones threatening or blackmailing a person using social media or spreading pornography on the web became a trend among the criminals. In accordance with a national daily, published on October 9, 2018 women are the biggest victims of rising cyber-crime in Bangladesh. If we evaluate why such kind of crimes are being committed so frequently then the thing we see is, It's easy to access, negligence, Lack of conformity in security process, weak gateway security, the unfamiliarity of technologies, the absence of proper filter etc. In last year a game called blue whale spread tension in the whole country. This kind of illegal games and many more issues of illegal trading as well as hiring hackers are available in Dark web and which is illegal and hidden. To access and transact into these illegal websites, one needs to have Cryptocurrency, which is the virtual money for the transaction on these sites

---

<sup>1</sup> <http://www.btrc.org.gov>

and in most of the countries cryptocurrencies are banned as well as Bangladesh. Bangladesh Bank said that "anybody caught using the virtual currency could be jailed under the country's strict antimoney laundering laws. Though the cryptocurrencies are almost untraceable and Do the government knows how much of these illegal currencies exist in Bangladesh? The statistics also show that only 5% conviction rate in cyber-crime cases over 5 years.

### **1.3 Rationale of the Study:**

Cybercrime has just turned into a going worry in both private and also open sector in Bangladesh. Amid the most recent decade private and open area has completed a revolution with the utilization of specialized improvement. Because of unapproved mediation to the system, company loses colossal classified data which caused a lot of financial lose. It has just been recognized that particularly Financial Institutions are in the most threading association for cybercrime that in the meantime reflects to the individual life. Some advancement accomplices has begun working how to handle cybercrime and improve effective communications .In the view above, it very well may be accepted that this report by and large will be useful for all concerned. Specifically, advancement accomplices will have the capacity to distinguish the how it affecting each field of our nation. People will have the capacity to end up mindful having thought how it impacts to human life. At long last, strategy producers will have an unmistakable thought on the effects of cybercrime to all fields that will empower to get ready and execute a comprehensive strategy or activity plan .The overall purpose of this research was to identify the impact of cybercrime in Bangladesh with regard to technological enhancement. The study has embarked upon the specific objectives are to assess:

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

The repeated failure of the prosecution and law enforcement agencies to prove allegations of cyber-crime has resulted in a paltry conviction rate of only 5% over the past five years, according to the records of the Cyber Tribunal (Bangladesh) in Dhaka. There have been only 16 successful convictions across 12 of the 236 cases heard before the tribunal since its inception in February 2013. In 129 of the other cyber-crime cases, the accused were cleared of all charges in the final report submitted before the tribunal by police. The tribunal discharged the accused in a further 59 cases without taking charges into cognizance, while the defendants in 36 cases were acquitted as the prosecution failed to prove the charges during the trial. Experts claimed the main reason the prosecution has been failing to prove allegations is their lack of knowledge on Information Communication Technology (ICT) and negligence.

#### **1.4 Research Questions:**

In my research paper, my most emphasized questions are as following,

1. Does the present legislation of Bangladesh is able to combat cybercrime?
2. Which kinds of Cybercrimes has commenced in Bangladesh so far?
3. Is the Banking sectors of Bangladesh are properly safe from cyber threats?
4. Is Digital currencies are legal to transact in Bangladesh? Is it traceable?
5. Does the Law enforcement has adequate expertise for Prevention?

#### **1.5 Objectives of the Study:**

The primary objective of the study is to make out the real scenario of cybercrime as well as:

1. To explain and examine the cyber-crime committed in different sectors;
2. To revisit the legal measures, strategies taken in Bangladesh as well as some other countries;
3. To explore existing schemes and mechanisms taken against cyber-crime in Bangladesh;
4. To analyze the problems regarding the scheme of the existing cyber legislations and
5. To make possible suggestions for the protection of cybercrime.

#### **1.6 Literature Review:**

In the words credited to the Greek Philosopher, Heraclitus, there is nothing permanent but change. These words, composed right around 2500 years back, are genuine today: we are living in a continually evolving world. The most fast pace of progress that we see is in the world of PC or the data and correspondence innovation. Over the last fifteen years, the expansion in innovation and the utilization of PC, in both the individual and business division has expanded amazingly. This innovation advance has guaranteed that the twenty first century is the data age. With every one of the conceivable outcomes that the new innovation offers for advancement and improvement, the same innovation can be utilized for malevolent and criminal purposes. Two or three years ago, fishing spelled with "F" was a lovely movement with an angling pole bar or a net where you could arrive yourself a decent feast for you and your family. Today, phishing, spelled with "PH" is an action with a phony site or email where one can arrive charge card or ledger details .We are to a great degree subject to the digital world for both our expert and personal work. With this developing reliance on data and correspondence technologies (ICT), there has risen new dangers to network and data security. There is an ever-developing weakness to cybercrime in this day and age. This is likewise evident for Bangladesh where the quantity of web clients is developing quickly and where ICT is important for the economy

This research paper is prepared in a manner only for Problem analysis and not focused on Recommendations. This paper shows legal ramifications against the latest cyber-crimes in Bangladesh and role of cryptocurrencies. Cryptocurrency is a digital-only version of currency. These types of currency are open source, this means that it is available to anyone, and peer-to-peer or, the capability for data to be transmitted from one computer to another without the need for a central server. Being peer-to-peer allows for shared access for all users, a level of amplified anonymity is generated here. There are many kinds of cryptocurrency, but the most widely used at the time of this writing is Bitcoin. Bitcoin is different from

other forms of cryptocurrency in the fact that it is totally and entirely decentralized. It compares to virtual cash that can be spent or traded online. Although Bitcoins are similar to online cash they do not have the ability to be fully anonymous like cash. Bitcoins are stored in a digital wallet once they are collected; this wallet is not necessarily tied to any definite person but it does have a Bitcoin address. The address or public key is recorded in what is called a block chain. This paper also emphasizes on how far the Bangladeshi cyber law has covered the latest cyber-crimes.

### **1.7 Research Gap:**

A few numbers of research has conducted on cyber security issues on Bangladesh and its impact but comparatively new sectors of cyber-crimes are not examined adequately. Most of these researches did not try to reach the roots deep within and elements are never eliminated. And I personally did not find any research on Digital currency and its use and abuses. The term cryptocurrency is a very new term for a country like Bangladesh. Effective researches and problem analysis can work as a precaution for the newest issues.

### **1.8 Methodology:**

The study is descriptive in nature. This study is done on the basis of secondary data. Secondary data is collected from magazines and research documents. Articles of newspapers and internet sources are also used. But the data were interpreted in light of the objectives mentioned above.

## **Chapter-2-classification of cybercrime and recent criteria's:**

Cybercrime is the most recent and maybe the most muddled issue in the digital world. "Cybercrime might be said to be those species, of which, sort is the customary wrongdoing, and where either the PC is a protest or subject of the lead comprising wrongdoing". "Any criminal movement that employments a PC either as an instrumentality, target or a methods for propagating further violations comes inside the ambit of cybercrime.

There are significant classes of criminal exercises with PCs:

1. Unapproved utilization of a PC. It might be submitted by taking a username and secret key, or by getting to the injured individual's PC by means of the Internet through secondary passage worked by a Trojan Horse program
2. Cybercrime might be perpetrated by making or discharging a vindictive PC program (e.g.; PC infection, worm. Trojan horse).
3. Cybercrime might be carried out by provocation and stalking in cyberspace.

All wrongdoings performed by maltreatment of electronic media or something else, with the reason for affecting the working of PC or PC framework. The followings are the best recorded sorts of cybercrime:

## **2.1 Hacking:**

Hacking is distinguishing shortcoming in PC frameworks or systems to abuse its shortcomings to get entrance. Case of Hacking Using secret phrase breaking calculation to access a framework Computers have turned out to be obligatory to maintain an effective organizations. It isn't sufficient to have detached PCs frameworks; they should be organized to encourage correspondence with outer organizations. This opens them to the outside world and hacking. Hacking implies utilizing PCs to submit fake acts, for example, misrepresentation, protection attack, taking corporate/individual information, and so on. Digital wrongdoings cost numerous associations a large number of dollars consistently. Organizations need to secure themselves against such assaults.

Programmers utilize an assortment of procedures for hacking, including:

- Powerlessness scanner: checks PCs on systems for known shortcomings
- Secret key splitting: the way toward recuperating passwords from information put away or transmitted by PC frameworks
- Bundle sniffer: applications that catch information parcels with the end goal to see information and passwords in travel over systems
- Satirizing assault: includes sites which misrepresent information by impersonating genuine locales, and they are in this manner regarded as confided in destinations by clients or different projects
- Root pack: speaks to an arrangement of projects which work to subvert control of a working framework from authentic administrators.
- Trojan Horse: fills in as a secondary passage in a PC framework to enable a gatecrasher to access the framework later
- Infections: self-repeating programs that spread by embeddings duplicates of themselves into other executable code records or reports
- Key lumberjacks: devices intended to record each keystroke on the influenced machine for later recover.

## **2.2 Virus Dissemination:**

Infection itself is programming that assaults other programming. It might cause for information misfortune, conclusion of transmission capacity speed, equipment harm and so forth. Trojan horse, Time Bomb, Logic Bomb, Rabbit are the vindictive programming.

## **2.3 Software Piracy:**

Software piracy is the unlawful duplicating, circulation, or utilization of software. It is such a productive

"Business" that it has grabbed the eye of sorted out wrongdoing bunches in various nations. As per the Business Software Union (BSA), about 36% of all software in current utilize is stolen. Software piracy causes huge lost income for distributors, which thusly results in higher costs for the shopper.

When you buy a business software bundle, an end client permit understanding (EULA) is incorporated to shield that software program from copyright encroachment. Commonly, the permit expresses that you can introduce the first duplicate of software you purchased on one PC and that you can make a reinforcement duplicate on the off chance that the first is lost or harmed. You consent to the permitting assertion when you open the software bundle (this is known as a therapist wrap permit), when you open the envelope that contains the software circles, or when you introduce the software.

Software piracy applies basically to full-work business software. The time-constrained or work limited variants of business software called shareware are more averse to be pilfered since they are openly accessible. So also, freeware, a kind of software that is copyrighted yet unreservedly circulated at no charge, likewise offers minimal motivating force for piracy.

Kinds of software piracy include:

- Soft lifting: Acquiring and introducing a duplicate of a software application from a partner.
- Customer server abuse: Introducing a larger number of duplicates of the software than you have licenses for.
- Hard-circle stacking: Introducing and offering unapproved duplicates of software on repaired or new PCs.
- Falsifying: Copying and offering copyrighted projects.
- Online piracy: Regularly includes downloading unlawful software from distributed system, Web closeout or blog. (Previously, the main place to download software was from a notice board framework and these were restricted to neighborhoods of long separation charges while on the web.

#### **2.4 Pornography:**

Cyber-pornography is the demonstration of utilizing the internet to make, show, circulate, import, or distribute erotic entertainment or vulgar materials, particularly materials portraying youngsters occupied with sexual acts with grown-ups. Cyber-pornography is a criminal offense, delegated making hurt people. One of the greatest broadcasted gets of kid sex entertainment culprits was propelled in May 2002 and called Task Metal. After the FBI got to the charge card subtle elements, email locations, and personal residences of thousands of pornographers getting to an English youngster erotic entertainment site, the particulars were given to the English police for examination. The capture of a PC expert in Texas prompted a universal examination that imprisoned Thomas Reedy for a long time for running the sex entertainment ring. Around 1,300 different culprits were likewise captured, including educators, tyke care laborers, social specialists, warriors, specialists, and 50 cops. Therefore, 40 youngsters, 28 of them in London, were put under defensive consideration. Police say that numerous youngster sex entertainment locales are kept running from Eastern Europe.

### **2.5 Credit Card Fraud:**

You basically need to type MasterCard number into www page of the seller for online exchange. On the off chance that electronic exchanges are not anchored the Visa numbers can be stolen by the programmers who can abuse this card by imitating the charge card proprietor. Through distortion of automated financial balances centers of taka might be misused. Now and again individuals are captured and charged for taking and abusing MasterCard numbers having a place with others.

### **2.6 Sale of Illegal Articles:**

Opiates, weapons and natural life and so on are sold by posting data on sites, sell off sites, what's more, release board or just by utilizing email correspondence. A considerable lot of sale destinations are accepted to offer cocaine for the sake of cash.

### **2.7 Online Gambling:**

Millions of sites are putting forth web based betting which are accepted to be real fronts of illegal tax avoidance. In spite of the fact that it isn't yet affirmed, these destinations may have association with medication trafficking.

### **2.8 Crimes against intellectual property:**

These include software piracy, copyright, violation, trademark infringement, computer theft source code etc.

### **2.9 Email Spoofing:**

A caricature email is one that seems to start from one source however really has been sent from another source. Individual Relationship might be endangered in view of email caricaturing. As of late, a part of the Worldwide Trust Bank encountered a keep running on the bank. Various clients chose to pull back the entirety of their cash and close their records. It was uncovered that somebody had conveyed ridiculed messages to a large number of bank's clients expressing that the bank was not doing so great monetarily what's more, could close activities whenever. The ridiculed email seemed to have begun from the bank itself.

### **2.10 Cyber Defamation:**

With help of PCs as well as the Web When any slander happens it is called digital criticism. It can discolor individual picture of any individual or notoriety of any organization, bank or foundation.

### **2.11 Cyber Stalking:**

Digital stalking includes following a man's development over the Web by posting messages on the announcement sheets frequented by the person in question, going into the talk room oftentimes by the person in question, continually assaulting the injured individual with messages and so forth.

### **2.12 Email Bombing:**

Email bombing can be submitted by sending immense number of messages to the unfortunate casualty bringing about the injured individual's email account (if there should arise an occurrence of an individual) or mail servers (in the event of organization or an email specialist organization) smashing. A large number of messages are sent to the individual record or mail server until it is slammed.



### **2.13 Data Diddling:**

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

### **2.14 Salami Attacks:**

For the commission of budgetary violations salami assaults are utilized. Here the significant thing is to make adjustment which is insignificant to the point that in a solitary case it would go totally unnoticed. "For instance a bank worker embeds a program, into the bank servers, that deduct a little measure of cash from the record of each client. No record holder will likely notice this unapproved charge, yet the bank worker will make a sizeable measure of cash each month.

### **2.15 REASONS OF CYBERCRIME:**

Hart in his work "The Idea of Law" has said 'individuals are helpless so guideline of law is required to ensure them'<sup>2</sup>. Applying this to the internet we may state that PCs are defenseless so guideline of law is required to secure and shield them against cybercrime.

The purposes behind the weakness of PCs might be said to be:

Ability to store information in similarly little space The PC has exceptional normal for putting away information in a little space. This stands to evacuate or on the other hand infer data either through physical or virtual medium makes it a lot less demanding. Simple to get to the issue experienced in guarding a PC framework from unapproved get to is that there is each probability of rupture not because of human blunder but rather because of the mind boggling innovation. By furtively embedded rationale bomb, key lumberjacks that can take get to codes, propelled voice recorders; retina imagers and so on that can trick biometric frameworks and sidestep firewalls can be used to move beyond numerous a security framework.

#### **Complex:**

The PCs deal with working frameworks and these working frameworks thusly are made out of a huge number of codes. Human personality is frail and it is absurd that there probably won't be a slip by at any arrange. The digital crooks exploit these lacunas and infiltrate into the PC framework.

#### **Negligence:**

Carelessness is firmly associated with human lead. It is along these lines truly likely that while securing the PC framework there may be any carelessness, which in turn gives a digital criminal to obtain entrance and power over the PC framework.

#### **Loss of evidence:**

---

<sup>2</sup> <https://www.questia.com/library/1446390/the-concept-of-law>

Loss of evidence is an extremely regular and clear issue as every one of the information are routinely wrecked. Further accumulation of information outside the regional degree additionally deadens this arrangement of wrongdoing examination.

## **2.16 Emerging criteria's and Impact:**

The vast majority focusing would expect that the expense of cybercrime has gone up lately. Yet, another report has put a number on it: Overall cybercrime costs an expected \$600 billion USD a year. That is up from \$500 billion USD in 2014, the last time security seller McAfee and research organization the Middle for Key and Global Examinations discharged a comparative report. The new gauge adds up to 0.8 percent of worldwide Gross domestic product, up from 0.7 percent in 2014.

"Cybercrime is constant, undiminished, and improbable to stop," composes report creator James Lewis, senior VP at CSIS. "It is simply too simple and excessively fulfilling, and the odds of being gotten and rebuffed are seen as being too low."

Inadequately secured IOT gadgets as a specific issue. Shaky IOT gadgets "give new, simple ways to deal with take individual data or access important information or systems," he composes. They additionally control botnets that can make gigantic forswearing of-benefit assaults.

Among alternate explanations behind the development in the expense of cybercrime:

Cybercriminals are grasping new assault innovations. Numerous new Web clients originate from nations with feeble cybersecurity. Online wrongdoing is getting to be less demanding through cybercrime-as-a benefit and different business schemes. Cybercriminals are ending up more monetarily modern, making it less demanding to adapt their endeavors. The Tor unknown program and Bitcoin are most loved instruments of cybercriminals. "Bitcoin has for some time been the favored money for dark net commercial centers, with cybercriminals exploiting its pseudonymous nature and decentralized association to direct unlawful exchanges, request installments from unfortunate casualties, and launder the returns from their wrongdoings," he composes. "Cybercriminals advantage from the way that no specifically distinguishing data is connected to the utilization and trade of Bitcoin, enabling offenders to work with close impunity." Tor engineers have safeguarded their venture by saying it shields clients' security by protecting them from corporate following and government observation. What's more, Bitcoin safeguards say the cryptographic money's unknown exchanges help enhance security.

The report assesses that PC and Web clients confront 80 billion malignant outputs every day. There are 33,000 phishing assaults and 4,000 ransomware day by day, with around 780,000 records lost to hacking. The report proposes a few stages to decrease cybercrime, despite the fact that security specialists have been pushing a few of the proposals for a considerable length of time.

## **Chapter -3-scenario of cybercrime in Bangladesh:**

### **3.1 State of Cyber Crime:**

The utilization of Web began in Bangladesh in 1993 out of the blue. It was opened for all on June 4, 1996 through the appointing of VSAT (Little Gap Terminal) association yet this presentation couldn't make a decent market at the specific beginning stage. After the year 1996, there were just two ISPs (Network access Suppliers) and around one thousands of clients in the nation. In any case, inferable from the fast development of this industry we had 180 ISPs by 2005. In 2006, Bangladesh got associated with Submarine Link (Ocean ME-WE 4 Submarine Link) which managed huge data transfer capacity and minimal effort than at any other time. <sup>3</sup>After this, throughout the years Bangladesh Media transmission Organization Restricted (BTCL) and Bangladesh Telecom Administrative Commission (BTRC) lessened the data transfer capacity cost at standard interims which pulled in an ever increasing number of clients towards the Web world. Starting at now BTRC (2014) has checked around three hundred and forty five or more enlisted ISP permit holders. <sup>4</sup>

The present government has announced the vision-2021. Inside 2021, this nation will wind up computerized nation and the per capital pay will be equivalent to a center pay nation utilizing IT divisions. In any case, the Administration and in addition different concerns consider cyber-crimes worriedly that are being perpetrated in this virtual world with the extension of Web and different systems which owes to change over this nation into a computerized nation.

In Bangladesh, cybercrime has drawn open consideration for the most recent few years. On August 23, 2004, an email was sent to a Bangla every day compromising to kill Sheik Hasina, the incomparable pioneer of a noteworthy political gathering. Following two days, on August 25, 2004, another email was sent to the Bangladesh police Home office issuing danger to Khaleda Zia, preeminent pioneer of another major political gathering, her senior child and a few individuals from parliament (Current Undertakings, 2014). It is troublesome for most confined clients of Data Innovation (IT) to comprehend the term „Cyber-crime“; Bangladesh is no special case. Here cyber-crimes began with spam sends and Trojan assault. Cyber-crime is expanding in Bangladesh step by step. Cybercrimes occur in Bangladesh mostly in the accompanying segments: (a) Cybercrime against people; (b) Cybercrime against property and money related foundations; (c) Cybercrime against associations; (d) Cybercrime against society; and (e) Cybercrime against national security.

In the time of 2013, the Skype discussion and blogging were the copying issues of our nation. Sex entertainment video and picture transfer occur in our nation all the time (Current Issues, 2014). Furthermore, extorting young lady by catching their naked photos is caused as often as possible by their beaus and others. Various people group sites have been presented, which the young ladies and young men are utilizing to trade telephone numbers for posting shrouded recordings or even pictures with bareness and so on. Hacking submitted into the Web record of Barisal DC office in 2003, the episode was uncovered after the DC office got an intensely enlarged Web bill and stopped a dissension with the Bangladesh Transmit and Phone Board (BTTB).

Hacking occurred in the site of Bangladesh Fast Activity Regiment (RAB) in 2008, when Programmers got to [www.rab.gov.bd](http://www.rab.gov.bd), the site read: "Hacked by Shahee\_MirzaHacking carried out into the mail of BRAC Bangladesh, the exchange report of Dhaka Stock Trade has been stolen through hacking ; crime

---

<sup>3</sup> Ahmed, Z. (2012) A Text Book on Cyber Law in Bangladesh, National Law Book Company, Dhaka.

<sup>4</sup> <https://www.dhakatribune.com/bangladesh/court/2018/01/30/conviction-rate-cyber-crime/>

perpetrated through embeddings exposed pictures to the site of Bangladesh National Parliament, embeddings stripped pictures to the site of Jamate Islami Bangladesh, embeddings bare pictures to the site of the Day by day Jugantor, Email undermining to World Bank Dhaka Office and contribution in cyber fighting with India and so on. Other than most as of late in 2014 and 2016, taking cash from Sonali Bank by hacking secret key and Bangladesh Bank heist recalls the savagery of cyber-crime in Bangladesh. Prior to 2013, there was cyber court just hypothetically not for all intents and purposes in Bangladesh. So in that period cyber-crimes were attempted by the session courts. In the wake of passing the ICT Demonstration in 2006, a couple of number of cases observed to be documented. In the ongoing days, a great deal of cases are being documented. Some of them are-(I) Four Blogger's case: four bloggers of Bangladesh in particular Asif Mohiuddin, Subrata Adhikari Shovu, Rasel Parvej and Moshiur Rahman Biplob were charged on 27th June, 2013 under group 57 of the ICT represent composing sick statement about Islamic religion and head administrator in the facebook and Online journals. (ii) Adilur Rahman Khan's case: Adilur Rahman Khan, Executive of "ADHIKAR" (Non-Government Human Rights Association), was charged U/S 57 (1), (2) of the ICT Act, 2006 and U/S 500 (c) and (d) of the penal Code,1860 on fourth September, 2013 for distributing report of fifth may of Hefajat development at Shapla Chattar, Matijhil, affirmed that the quantity of dead body detailed by "Adhikar" is 60 (sixty), was false and planned to debase the notoriety of the Govt, to instigate the muslims, to hamper the notoriety of the State to the remote states. (iii) Mahmudur Rahman Khan's case: the editorial manager Mahmudur Rahman Khan and Distributer Hasmata Ali of the everyday paper "Amar Desh" were charged U/S 56 and 57 of the ICT act, 2006 and segments 124, 124 (a), 505 (a), 120 (b) and 511 of the Penal Code ,1860 for distributing the Skype discussion between equity Nijamul Haque Nasim (the then Administrator of international war crimes tribunal 1) and his Belgium companion Dr. Ahmed Jia uddin on thirteenth December, 2012 (Ahmed, 2014). In this manner cyber-crime is the principle concerning issue of Bangladesh government today.

Moreover, PC proficiency in Bangladesh is consistently on the ascent. There is additionally a developing number of Web clients; mobile phone is across the board as is availability of innovation like SMS. While even a couple of years back PCs were incomprehensibly utilized as advanced 'typewriters', they are presently being utilized to keep up records worth a huge number of takas and all the more imperatively, in putting away helpful data.

It is foreseen that the progressive move by the present government to digitalize Bangladesh will fundamentally quicken enhancements in this segment. This difference in viewpoint towards data innovation is bringing ease, freedom, development and enhancement in our Bangladeshi lives. In any case, in the midst of this desire for another future, a developing danger prowls in obscurity – the universe of cybercrime.

Cybercrime is a dark word for most remote clients of data innovation (IT). This is as valid in Bangladesh for what it's worth in whatever remains of the created countries. This is anyway a noteworthy worry for individuals engaged with IT.

Mindful of the danger or not, ordinary a huge number of clients are being vulnerable casualties of cybercrime.

Be that as it may, this is nothing new to the extent wrongdoings are concerned; just the shape has changed. At the point when innovation is used to take or degenerate data, utilized for double dealing or extortion, or for any customary lawful offense so far as that is concerned, it is named as cybercrime.

As opposed to taking cash straightforwardly, all things considered, cybercriminals hack into servers of banks, utilizing PCs or cell phones, and exchange substantial measure of cash to different records. Rather

than taking records from workplaces, they split into PCs and remove important data. Acquainting infection with an outside PC to wipe out memory is an offense, much the same as incendiarism. Basically the violations as comparative, just the structures are different.

This wrongdoing is regularly dedicated by novices, rather energetically; some are known to have been executed out of competition, desire and furthermore for financial advantages. The cases which have been made open in Bangladesh were for the most part done by a type of non-experts for whom hacking/breaking is a negligible pastime. In the most recent two years, there have been real instances of cybercrimes in presumed associations engaged with its field however stayed avoided people in general eye to keep up the constructive picture of the associations; clients of the concerned organizations were likewise left in obscurity.

The risk is apparent. The examples saw in Bangladesh have additionally been seen somewhere else in their underlying stage, where cybercrime is presently a noteworthy danger to trade and living. Everyday remote clients are falling prey to infection assaults, misrepresentation, exchange and defilement of data and different malice. Thinking about the social and related harm, the misfortune is enormous. Obviously, just cases with significant impact to the economy, budgetary exchanges and legislative issues have gone under the spotlight.

In Bangladesh a significant number of cybercrime have gone under open consideration over the most recent couple of years. Unknown demise dangers to Sheik Hasina, the then Pioneer of the Resistance, dangers by and large through messages, hacking of sites kept running by law authorizing organizations and slander of private data of regarded and mainstream people of the nation are a portion of the instances of cybercrime in Bangladesh.

Clients of data innovation are falling prey to cybercrime frequently. With no earlier learning they are being enrolled in online studies, once in a while turning into a pawn to violations of a more genuine nature. Without the vital arrangements for counteractive action or even recognition, they stay undocumented much of the time.

Consistently cybercrime adds up to a few billion dollars of monetary harm. Famous organizations regularly measure the worldwide effect of cybercrime and as per PC Financial aspects the money related harm, globally, in 2006 alone, has been over 13.3 billion dollars. As the outside world is more subject to IT, the impact of cybercrime is more articulated in the Western World. AS far as monetary misfortune is worried there has, up until now, not been any genuine wrongdoing including IT in Bangladesh. One must remember that money related issues here are not as subject to innovation similar to the case in the outside world. <sup>5</sup>We additionally come up short on the expected mastery to consider the financial set back caused by cybercrime.

So there is no extension for us to relax. Analyzing cases experienced in the West we can survey the plausible monetary misfortune we may involvement. The time has come when one should play it safe for battle this developing peril at general society, private or even on an individual dimension. Data innovation is a device that we as a whole should grasp; there is no extent of denying its quality or impact around us.

As of late IT the board Relationship of Bangladesh as a team with Bangladesh Police, masterminded a two-day workshop of cybercrime. High authorities of the police, alongside the real partners of the IT

---

<sup>5</sup> Reza, Y. & Azim, R. (2009) „Cyber-crime and prevention measure: Bangladesh perspective“, Daily Star.net/law, 5th September, Law and our Rights, p. 15

Segments were available in the meet. It was acknowledged through discourse that obliviousness remains the most serious issue of the undertaking at the private, institutional and even the national dimension. To add to this, there is an absence of present day Digital Law, the absence of mastery of the law authorizing offices, the nonattendance of key tech apparatuses, the nonexistence of the required foundation at the institutional and national dimension, and a lack of inspiration, also the indiscreet demeanor of the distinctive associations included straightforwardly in this segment, to be specific ISPs and Telecoms.

For the remote clients, utilizing an enemy of infection programming, setting up a firewall and some other security tips will get the job done as a prepare for cybercrime. The test lies at the authoritative and state level. To battle this test, the law, the framework and the labor must be very much joked to address the current issue. Similarly as we should manage the entry of data, the matter of opportunity of data must be borne as a primary concern. While building up an approach or structuring a framework one must ensure that each data esteemed important for the client must be effectively available while the data, to which the client has no lawful right, must be painstakingly covered up.

As of now, what is required is a very much figured Digital Law. With the changing framework and the evolving conditions, this law must be confirmed and stayed up with the latest. It is apparent from concentrate the drafting of digital laws of created and some creating countries that creation due thought to the overarching framework of the nation is crucial. In these nations, there has been impedance from the state to compel certain infrastructural alterations in private ventures engaged with IT.

Keeping these two contemplations our neighboring nation India has shaped a Digital Law that is viewed as current. In 2000, the digital law was first drafted as an augmentation of the Data Innovation Law. At first covering just fundamental violations referenced in the Reformatory Code, the law was slowly changed to incorporate laws exceptional to cybercrime. Another issue that was viewed as imperative in the workshop was the gathering of information and proof of a wrongdoing that has been submitted and its evidential incentive in lawful procedures.

The matter of infrastructural improvement and usage of law comes inseparably with drafting of the law. This requires an intensive thought of our current circumstance at the private and open dimension and joining changes as need be. Each part of administration giving – server, stockpiling, arrange and so forth.) — must be produced in understanding to the rules and the digital law. It is accordingly imperative that both open and private divisions are very much aware of the predominant benchmarks in this field.

The law implementing offices must be furnished with the most recent innovation essential for battling violations identified with data innovation; the legislature should likewise grant scholastic learning amid preparing of officers of law implementation. There must be collaboration with universal volunteer associations and different specialists of this field to pick up mastery in the fight against cybercrime. Except if vital advances are not taken now, it will demonstrate difficult to attempt cybercrime in the official courtroom.

### **3.2 IMPACT OF CYBERCRIME AGAINST THE GOVERNMENT:**

Cyber terrorism mongering is one particular sort of wrongdoing in this classification. The development of web has demonstrated that the mode of the internet is being utilized by people and gatherings to undermine the universal governments as additionally to threaten the subjects of a nation. This wrongdoing shows itself into fear mongering at the point when an individual "splits" into an administration or military looked after site. In a report of it was said that web was turning into a shelter for the psychological oppressor associations.

### **3.3 Cyber terrorism against the government organization:**

At this point a need might be felt that is the need to recognize digital psychological oppression and cybercrime. Both are criminal acts. Anyway there is a convincing need to recognize both these wrongdoings. A digital wrongdoing is commonly a local issue, which may have worldwide outcomes; anyway digital fear mongering is a worldwide concern, which has household and additionally global results. The normal type of these psychological oppressor assaults on the Web is by disseminated disavowal of administration assaults, detest sites and despise messages, assaults on delicate PC systems, and so on. Innovation astute fear mongers are utilizing 512-piece encryption, which is by Incomprehensible to unscramble. The ongoing precedent might be referred to off – Osama Canister Loaded, the LTTE, and assault on America's armed force sending framework amid Iraq war. Digital psychological warfare might be characterized to be " the planned utilization of problematic exercises, or the danger thereof, in the internet, with the aim to advance social, ideological, religious, political or comparative goals, or to threaten any individual in facilitation of such targets".

Another definition might be endeavored to cover inside its ambit each demonstration of digital psychological oppression. A fear based oppressor implies a man who enjoys wanton murdering of people or in savagery or in disturbance of

Administrations or methods for interchanges fundamental to the network or in harming property with the view to –

- (I) putting people in general or any segment of the general population in dread; or
- (ii) influencing antagonistically the amicability between various religious, racial, dialect or provincial gatherings or ranks or networks; or
- (iii) constraining or overawing the legislature set up by law; or
- (iv) Imperiling the sway and honesty of the country and a digital psychological militant is the individual who utilizes the PC framework as a methods or finishes to accomplish the above goals. Each demonstration done in compatibility thereof is a demonstration of cyber terrorism warfare.

### **3.4 Cybercrime scenario in Banking Sector of Bangladesh:**

In past few years the Banking sectors has gone through serious security breaches:

- On January 6, 2013 Islami bank Bangladesh was hacked by Mind cracker.
- In 2015 a private bank was hacked and faced unauthorized money withdrawal.
- On December 2, 2015, Hackers breached the network security of Sonali Bank and took control of its website for a couple of hours. The programmer distinguished himself as a 'Muslim Hacker'.
- In February 2016 six ATM booths was skimmed attacked any three commercial Bank was also affected.

- Furthermore, the biggest e-illegal tax avoidance in the historical backdrop of keeping money happened in February 2016, when programmers stole \$101 million from the Bangladesh ledger's with the Federal Reserve Bank of New York.<sup>6</sup>

Proof of hacking in business banks exhibits debasement in the administration's obtainment structure where inadequate sellers were chosen without legitimate assessment of abilities and counsel of IT specialists. The disillusioning part of this event from the Bangladesh Bank was that, while giving vital exhortation to all concerned, they had neglected to regard their own proposals and fail to take attractive wellbeing proportion of their own organization and its association with other related monetary accomplices abroad, which lead to the biggest e-tax evasion in the saving money area of Bangladesh.

### **3.5 Case study 1: ATM card skimming**

The underlying stunt came after the disclosure and objections recorded due to maltreatment of ATM machines fitting in with a few banks and withdrawal from different private records of a considerable measure of money without endorsement of the record holders.<sup>14</sup> People were captured by the police on 4 Walk, 2016. It included 12 remote nationals who were people from overall digital wrongdoing misrepresentation group. They had misleadingly used web based systems administration media moreover hacked data of individual customers. Skimming is a method used by advanced offenders to copy singular data from the attractive strip on an ATM card. The criminal fits a skimming gadget in the card opening of ATM corner. When a card is swiped through a skimmer, singular information contained on the attractive strip is examined and set away on the device or transmitted remotely to the offenders. With the card data, they can lead value based deception, make new cards with the stolen character and individual information, or offer the cardholder data on the secret market. The frustrating part of this event from the Bangladesh Bank was that, while giving vital exhortation to all concerned, they had neglected to regard their own recommendations and fail to take attractive wellbeing proportion of their own organization and its association with other related monetary accomplices abroad, which lead to the biggest e-tax evasion in the managing an account segment of Bangladesh.<sup>7</sup>

### **3.6 Case study 2: Bangladesh Bank Heist**

In February 2016, the taking of \$101 million from the stores of the Bangladesh Bank has brought up issue on the introduction of money related foundations to digital wrongdoing gatherings. This occurrence have tested the capacity of existing components in anticipating such episodes. Additionally, this robbery meant the requirement for reinforcing the worldwide co-task in handling digital wrongdoing. The programmers recovered the national bank's exchange codes and sent installment exchange demands worth \$1 billion to the Central Bank of New York. They asked for the assets of Bangladesh be exchanged to a bank in the Philippines. From that point, the money was exchanged to no less than three Pilipino gambling clubs: At the clubhouse, somebody changed over the money into chips for wagering and afterward reconverted the chips into money. This cash was then sent to ledgers in Hong Kong. An extra reserve of about US\$ 21 million was likewise exchanged unlawfully to an outsider in Sri Lanka. The endeavor couldn't be satisfied in totality following a composing mistake that alarmed one of the steering banks and exchange was ceased. . Rather than "establishment" the programmers had spelt it as "fandation". This provoked a directing Bank Deutsche Bank to look for elucidation from the Bangladesh Bank, which ceased the exchange. Spelling botch kept the illicit moving of cash. Yet, the programmers were effective in siphoning \$81

<sup>6</sup> :<http://www.risingbd.com/english/cyber-crime-inbangladesh-a-growing-threat-in-digitalmarketplace/28940>

<sup>7</sup> :<http://bdnews24.com/business/2016/02/14/cardskimming-at-six-atm-booths-from-three-banks>



million in the underlying four exchanges. The robbery of such an expansive sum from national stores amazed numerous in Bangladesh and abroad. Questions are being communicated about the nation's status to secure its monetary foundation, which is experiencing digitization. Diverse examinations are being conveyed by different enquiry commissions like FBI, Bangladesh Banks named board and CID authorities of Bangladesh. Bangladesh specialists have distinguished something like 20 outside nationals who they guaranteed were associated with the digital heist till date.<sup>8</sup>

## **Chapter-4- Status of Legal Mechanism and Ramifications**

### **4.1 National legislative framework:**

The United Nations Commission on Web Exchange Law (UNCITRAL) received as the Model Law on Electronic Business in 1996. The Model Law gives that all Nations should offer thought to it when they sanction and modify their digital laws. The Model Law accommodates square with legitimate treatment of clients of electronic correspondence and paper based correspondence.<sup>9</sup> Thus the establishments of Bangladesh in such manner are the National ICT Policy 2009, planning Data Innovation (Electronic Exchanges) Act (ITETA), 2000. It is to be noted here that ITETA is by all accounts a nearby copy of the Indian IT Act-2000 that neglected to incorporate issues like digital crouching, spam and digital fear based oppression. The Data and Communication Technology (ICT) 2006 has been authorized dependent on the said Model Law and come into power on eighth October-2006 and ICT leads in 2010 to encourage electronic trade and empower development and improvement of data technology. It incorporates the arrangements of bringing the digital culprits inside the ambit of criminal purview. The ICT Act was corrected in 2013. This Demonstration stretches out to the entire of Bangladesh as well as applies to offenses and repudiations submitted outside Bangladesh (Sec.4 of the ICT act, 2006). It has 90 areas partitioned into 10 sections. A digital unfortunate casualty in Bangladesh has a superior chance to get the best possible cure under the ICT act, 2006. This rule is the first and the main entryway open for the legitimate cure of various digital wrongdoings in Bangladesh. Through this resolution, it is being endeavored to find all the plausible cases and grounds and give punishment for digital wrongdoings often happening at present and which may happen in future. Some significant inquiries are raised with respect to the particular idea of carrying out digital wrongdoing and as to no treating digital wrongdoing and digital common wrong independently. As of late, Digital Security Act, 2016 as a supplemental to the ICT act, 2006 is received by the Bureau which anticipated that would make a solid lawful system to battle digital wrongdoing in Bangladesh. This demonstration has 45 areas partitioned into seven sections which enable Government to build up National Digital Security Organization (NDSA) headed by an Executive General. With a view to anchoring, forestalling and controlling digital criminal exercises, NDSA is approved to screen, watch and make important strides in regard of all the Bangladeshi PCs or advanced frameworks, systems, mobiles or computerized communication (voice and information) systems and so forth. NDSA for this reason can build up advanced criminological lab for digital measurable investigation and it can likewise set up Bangladesh Digital Crisis Reaction Group (Bangladesh-CERT) for speedy reaction against digital wrongdoings (Sec 5 of the Digital Security Act, 2016).

In addition, there will be a National Computerized Security Chamber (NDSC) led by the head administrator to discuss digital related issues and take quick choices (Section 6 of the Digital security Act, 2016).<sup>10</sup> This Demonstration likewise makes every one of the arrangements of the Proportional Co-task

---

<sup>8</sup> <https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8#axzz46NHKzCwH>

<sup>9</sup> The UNCITRAL model law on electronic commerce (1996).

<sup>10</sup> BTRC website (2014) viewed March 2014, <http://www.btrc.org.gov>

relevant to examine, arraign and settle the trans-more extensive offenses in the topic of territorial and worldwide participation (Sec 39 of the Digital security Act, 2016) and every one of the Offenses submitted under this demonstration have been made triable under the digital council and digital reappraising court built up under the ICT act, 2006.

Bangladesh Government has set up a unique council under the ICT act, 2006 called „Cyber Tribunal“ at Dhaka in 2013 to deal with cybercrimes that incorporate falseness, blackmail and the hacking of PC framework on-line. The move came after the UK-based financial expert asserted that it had recorded 17 hour discussion on Skype and 230 messages between the „International war crimes tribunal 1“ Executive and Bangladeshi exile in Brussels. The „International war crimes tribunal 1“ Director, Equity Md. Nizamul Haque, surrendered his situation in the midst of contentions over his discussion with the exile Ahmed Ziauddin (Bangladesh Shangbad Shangstha, 2013).

The law service issued a newspaper notice on the foundation of the council on January 28, 2013 under the Data and Correspondences Innovation Act 2006 in Dhaka to only arrangement on-line wrongdoings in an expedient way. At first, one court was set up in Dhaka covering the entire of Bangladesh in spite of the fact that the law stipulates that at least one digital councils could be set up for a powerful and quick preliminary of criminal activities carried out on-line (Bangladesh Shangbad Shangstha, 2013). Cyber tribunal, the first of its sort in the nation, will be enabled to finish up preliminaries inside a half year. A few hundred of protests have been documented before this court and the preliminary of those are in pending.

Arrangements for setting up digital court and digital redrafting council having unique and re-appraising locale individually and disciplines of lighter/extreme shape, preliminary methodology and so forth have been given by the ICT Act, 2006 (Sec. 82 and 84 of the ICT Act, 2006). Yet, it is worth-referencing here that the ICT Act, 2006 isn't comprehensive enough to ensure this tremendous the internet and IT industry. Notwithstanding the use of the arrangements of the ICT Act, a great number of procedural and basic obstacles are being confronted which are as per the following:

#### **4.2 Absence of Specialized Master:**

Judges and the legal counselors of digital council or session Courts (Sec. 68 (2) of the ICT Act, 2006) are the specialists of laws, not of innovation, all the more explicitly of Web innovation. So the judges of digital court and also digital re-appraising council (Sec. 82 of the ICT Act, 2006) have the chance to be helped by the ICT master. Yet, is it conceivable to give the decision based on another's learning? The truth in the Act is that so far no arrangements exist stepping up with regards to the Administration to prepare up the judges for obtaining the base innovative learning required for guaranteeing equity. The Computerized Security Act, 2016 additionally neglected to underline on this issue.

#### **4.3 Lack of knowledgeable law enforcers:**

A police officer not below the rank of a Sub-Inspector can be the Investigation Officer regarding the cyber-crimes (Sec. 69 of the ICT Act, 2006). Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of cyber tribunal and cyber appellate tribunal.

So, is it possible for such a police officer to make a proper investigation into such matters? Moreover, it may result in a snag to justice.

#### **4.4 Procedural Difficulties:**

The Government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of the tribunals (Sec. 82 of the ICT Act, 2006). Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state in this regard.

#### **4.5 Lack of Clearance of the Terms:**

The cyber-crime related terms have not been defined in this Act such as data diddling, tempest attack etc. For which existing law suffers from proper application.

#### **4.6 Lack of Sufficient Laws:**

No clear provision included in the Act for bringing the cross broader cyber criminals under the jurisdiction. Besides, No Cyber forensic laws exists which is badly needed to formulate for proper cyber investigation and inquiry.

#### **4.7 Civil-Criminals Difficulties:**

No distinction made for cyber-crime and cyber civil wrong which results the compensation and damages demand problems.

In this above situation, Bangladesh Government recently adopted Digital Security Act, 2016 to overcome those lacunas and give effective measures thereof. Bangladesh police creating special cyber unit brings the cyber criminals under control. After a long period of unanimous attack of cyber warriors between Bangladesh and India, Bangladesh Government has opened a new website to defense cyber-crime as Computer Security Incident Response Team (BD-CSIRT) for cyber security service. This team is named as Bangladesh Cyber Emergency Response Team (Bangladesh CERT) in the Digital Security Act, 2016.

#### **4.8 Provincial Systems and the Status of Cyber Law:**

Cyber law covers a wide assorted variety of political and legitimate issues identified with the Web and other correspondence innovation securing licensed innovation, protection, opportunity of articulation in one's locale. It additionally inspects the cyber related laws of SAARC nations, USA, Australia, Japan, and European and comparable enactments. Abroad territorial nations around the globe are elevating worldwide measures to bargain properly with cyber wrongdoing for the development of media communications, PC organize. One of them is the Hyderabad Assertion (2004) which announces that blending the legitimate and authoritative structure for creating trust in online business exchanges crosswise over Asian nations. In view of UNCITRAL Show Law (1996), neighboring nation India ordered numerous cyber related laws, standards and directions for insurance ICT advancement parallel with different areas. The Indian Data Innovation (ITA) Act-2000 was the initial move towards data innovation security in the nation and endeavors to enhance the idea of electronic administration and web based business. The Indian Parliament got the Semiconductor Coordinated Circuits Format Plan (SICLD)

Act, 2000 after the consent of the President on the 4 September 2000 and the other IPR Act .The Patent Demonstration, Exchange Imprints Act, and Copyright Act and so on. <sup>11</sup>

Cyber related or cyber wrongdoing enactments are still despondently missing in Africa, the Center East, Asia and Oceania. Mechanically and exceedingly created nations, particularly those in Europe and North America have cyber related laws and cyber wrongdoing laws to ensure and spare their security, PC, PC system and Web. Some creating nations are currently taking activities in this regard. Worldwide Techniques and the Status of Cyber Law Global law, traditions, two-sided and multilateral bargains have not been created for Web separating and administering the cyber wrongdoing. The European Tradition on Cyber Wrongdoing came into power in 2001. The European Tradition on Cyber Wrongdoing, 2001 is the first historically speaking global arrangement on criminal offenses carried out against or with the assistance of PC systems, for example, the Web. After Joined Countries convention on cyber security and cybercrime, The Unified Countries Office on Medications and Wrongdoing (UNODC) has distributed a useful guide. The rule underlines on the utilization of the Web for fear based oppressor purposes among part states for increasingly successful examination and arraignment of psychological oppressor cases including the utilization of the Web. Ground-breaking nations including USA, England, China, Russia, Philippine and a significant number of the nations are considering and getting ready law to ensure the cybercrimes.

#### **4.9 Global Laws and Traditions on Cyber Law:**

Global law gives couple of clear apparatuses to break down Web sifting, through the potential surety exists (The Unified Countries Tradition on the Utilization of Electronic Correspondences in Worldwide Contracts, 2005). Nations regularly make law through multilateral assertions that bear on Web law and direction. For example, exchange assertions habitually incorporate arrangements identified with licensed innovation that could influence sifting issues. An up and coming age of global helpful law, some have contended, may likewise incorporate assurances for access to correspondences. The European Tradition on Cyber-crimes 2001: The European Tradition on Cyber Wrongdoing 2001 is the main ever worldwide settlement on criminal offenses carried out against or with the assistance of PC systems, for example, the web. The Clergymen of outside Undertakings at last received the Tradition on November 8, 2001. The Tradition on cyber wrongdoing was opened for mark in Budapest, Hungary on November 23, 2001. Pastors or their delegates from the 26 individual Part States marked the bargain. The aggregate number of signatories is 43. By marking this arrangement, part nations concurred on a typical stage for trade of data identifying with examination, arraignment and the methodology against cyber wrongdoing, including trade of cyber lawbreakers.

#### **4.10 Other Worldwide Methodologies:**

A portion of the universal associations have acknowledged and perceived trans-fringe nature of cybercrime and the requirement for global harmonization of specialized, lawful and different arrangements. The principle of them in this field are the Association for Financial Participation and Advancement (OECD), the Board of Europe, the European Association, G-8 and the Interpol. Moreover, the UN, World Licensed innovation Association (WIPO) and General Concurrences on Exchange and Tariffs (GATS) have likewise assumed an essential job. These associations have fundamentally added to

---

<sup>11</sup> The Indian Information technology Act (2000).

the harmonization of criminal law and additionally of common and authoritative law in the majority of the territories of PC related law change. The primary extensive investigation into the correctional law issues of PC related violations on global dimension was started by the OECD. The OECD completed from 1983 to 1985, an investigation of the likelihood of a universal harmonization of criminal laws to address PC related wrongdoings (Joined Countries Manuel on the Avoidance and Control of PC Related Wrongdoing, 1995). The examination announced in 1986, on reviewing existing laws and proposition for change and prescribed a base rundown of maltreatment, that nations ought to consider punishing by criminal law.<sup>12</sup>

#### **4.11 Cyber Laws in other Developed countries:**

Innovatively much created nations, particularly those in Europe and North America, Australia, South Korea, Singapore, Japan have digital related laws and digital wrongdoing laws to secure and spare their protection, PC, PC system and Web. Some South American nations have digital laws that keep a few classifications of digital wrongdoing, however others have basically no digital laws set up. Regulatory, corrective and common enactment was established to ensure information against illicit access to PC framework and related citizens' rights to security. The accompanying nations ordered their digital laws; Sweden in 1973 and 1986; the Unified Conditions of America in 1974, 1980 and 1984; Denmark in 1978 and 1985; Austria in 1978 and 1987; France in 1977 and 1988; Japan in 1997 and 1988; Spain in 1992 and 1995; Italy in 1978 and 1997; Greece in 1988 and 1997; and Malaysia in 1997; and so forth. U.K., USA, India, Malaysia and some other created nations have set up unique wings of police to battle the digital wrongdoing. On the last 23rd July of 2009, North Korea turned Korea Web and Security office, an administration office joining three of its previous Web innovation associations. Presently, this organization will try to make North Korea a more grounded and a safe propelled nation in utilizing Web. India and some different nations have additionally made such offices.<sup>13</sup>

#### **Chapter-5- Bitcoins and the Future of Cryptocurrencies in Bangladesh:**

Bitcoin is a digital currency and an overall installment framework that capacities on the block chain innovation. The freely dispersed record made by block chain innovation requires a digital currency to lead exchanges. Bitcoin is one of those digital forms of money. While there are numerous digital currencies accessible for use, bitcoin has risen as the most prevalent around the globe. On the off chance that bitcoin is to be viewed as a money like the Bangladeshi taka, we would need to realize how to utilize it. The clients of bitcoin require wallets for putting away their coins. The wallets can be physical—a little equipment gadget, or programming based—put away in a PC. In either case, the money must be put to utilize by means of PCs associated with the Web. Further, cell phones can function as substitutes for PCs.

---

<sup>12</sup> Walker, C. & Akdeniz, Y. (1998) „The governance of the Internet in Europe with special reference to illegal and harmful content“, Criminal Law Review, Crime, Criminal Justice and the Internet, Cyber Law Research Unit, Centre for Criminal Justice Studies, Department of Law, University of Leeds, available at [www.cyberrights.org/.../CrimLR\\_ya\\_98.pdf](http://www.cyberrights.org/.../CrimLR_ya_98.pdf)

<sup>13</sup> Weimann, G. (2004) „Cyber terrorism how real is the threat, special report“, United States Institute of Peace, Washington,

Clients can select to keep a piece of the record with them in their PCs on the off chance that they plan to perform complex exchanges. The clients can likewise assume the job of exchange verifiers. In the realm of bitcoin, such clients are called excavators. Diggers confirm exchanges and vote to approve them and make the sections changeless. Diggers are typically remunerated by bitcoins crisply mined out of the framework subsequent to satisfying predefined criteria, and the sum is controlled by the PC calculation. The job of bitcoin excavators covers with that of national banks in a few territories. For instance, we have national banks to print and issue monetary standards in our current financial framework. Their guarantee of a cash bearing a specific esteem is typically ensured by the legislatures supporting them. Thus, the national banks appreciate the benefit of printing cash and overseeing swelling as per their financial goals. In the realm of bitcoin, this is the activity of a PC calculation. National banks are approved by the rules of their nations. Bitcoin looks to decentralize some portion of their job among the overall population spread crosswise over various nations. Bitcoin additionally means to make swelling unsurprising by giving the calculation a chance to mine and make new coins. Thus, the danger of significant worth devaluation because of expansion is limited. Without precedent for the long history of fiat cash, bitcoin has effectively shown that money direction can be decentralized and democratized—an insurgency that would not have been conceivable without the fundamental advances. In any case, there are sure restrictions on the usefulness of bitcoin. National banks deal with the supply of cash utilizing different monetary strategies, for example, financing costs, with the point of catalyzing monetary development and monitoring ware costs. Bitcoin comes up short on that highlight because of its decentralized structure and algorithmic control. The aggregate supply of bitcoin today is evaluated to be around 16.80 million, as per different assessments. Its supply is expanding each day yet is restricted by the pace of mining, and can increment up to 21 million. Subsequently, its cost increments in the money trades relying upon the pace of its notoriety and request. Contrasted with this, the supply of the taka (M1) is about 2.27 trillion in esteem, as indicated by the site information of Bangladesh Bank. The national bank can increment or decline its supply to oversee monetary parameters.

The constrained supply of bitcoins limits its viable use in regular day to day existence. Everyday life requires cash in intelligible units, with satisfactory supply and open acknowledgment. National banks carry out this activity for their own monetary standards inside their purviews. Bitcoin needs to develop with innovative progressions and assemble these characteristics after some time. Given the high cost of bitcoin, it might be viewed as a product, for example, gold, silver or different valuable metals whose supply is restricted. The costs of items are cyclic in nature—they rise and fall in the market. For quite a long time, wares like gold or silver have turned out to be of extraordinary incentive because of their open worthiness as assets. Then again, bitcoin has been operational for pretty much nine years and it is too soon to remark on its long haul prospects. Over the world, the notoriety of bitcoin has been expanding. It is additionally being utilized for monetary exchanges. This makes difficulties identifying with the implementation of laws. Because of bitcoin's borderless character, law authorization offices are attempting to screen unlawful exercises including bitcoins. Bitcoin isn't perceived as lawful delicate in numerous nations and seems to be, along these lines, not appropriate for use in purchasing or moving exercises. Expense specialists are partitioned on whether a bitcoin exchange is a money exchange or an item exchanging. Controllers may set aside some greater opportunity to make up for lost time with this innovative progression. With progressions in innovation, digital currencies are bound to end up the standard cash for exchanges in the coming years. National banks may choose to circle their very own cryptographic forms of money with their exclusive calculations and controls and may decentralize the administration of digital forms of money among the general population through a mutual record while holding some administrative controls with themselves. On the other hand, they may choose to underwrite bitcoin alongside a few systems for cross-outskirt coordinated effort and financial control.

### **5.1 Un-traceability and potential threats:**

Bitcoin is adequately a third cash, sitting close by platinum cards and customary money. It may be absolutely computerized however Bitcoin is ending up increasingly more mainstream constantly, with soaks rises each year in its usage.

With an ever increasing number of individuals utilizing Bitcoin consistently the advantages and dangers develop nearby it. Bitcoin isn't exactly as straightforward as going into a shop and giving over some cash or checking your card however it's not as unpredictable as it may show up either. But before you approach purchasing and exchanging Bitcoins it's dependably a smart thought to peruse up on the advantages and dangers included. Regardless of whether you're knowledgeable in how Bitcoin functions an update on the principle advantages and dangers is dependably a decent idea. The namelessness and un-detectability of Bitcoin as the abnormal refinement of being both an advantage and a hazard. One of Bitcoins establishing standards was that it was to be totally unknown to prevent associations or gatherings from following your assets. What's more, not normal for holding cash retained there are no long hold up times or complex sending and accepting techniques, the detectability likewise keeps government outlets from swindling you. However, un-discernibility means that utilizing Bitcoin to buy illicit materials like medications is a probability, truth be told, a few governments have prohibited Bitcoin because of its capability to pull in criminals. Bitcoin may develop in notoriety year on year yet the commercial center hasn't actually rushed to adjust to this new advanced money. While an expected 100,000 better places acknowledge Bitcoin as an installment strategy a significant number of these are electronic stages only. This probably won't be a major issue because of the expansion in computerized shopping, however it limits the quantity of spots you can really utilize your Bitcoins to purchase things. Bitcoin may be extremely prevalent right now and worth a great deal yet who knows what's on the horizon? Another contending money could rise in future which greatly impacts the esteem and ubiquity Bitcoin is currently encountering. The present unpredictability of Bitcoin likewise implies that it is troublesome for a few outlets to acknowledge them as payment. Bitcoin is a computerized cash which implies it as every one of the advantages and disadvantages of being advanced, while this makes Bitcoin quick when making exchanges online it has a few issues. Most eminently is the potential for hacking and different cybercrimes and because of the namelessness of Bitcoin finding who precisely hacked or misled you is unbelievably troublesome, if not impossible. Bitcoin is the principal computerized money and as observed a major ascent in its ubiquity since its presentation in 2009. Numerous individuals today are putting resources into Bitcoin but since of its instability, there's no real way to know without a doubt how those speculations will pay off. But what we can be sure of is that it as various advantages: it's quick, untraceable, unknown and decentralized making it emerge from the other installment strategies accessible today. There are dangers to know about and it's not acknowledged all over the place.

### **5.2 Illegality of bitcoins and Law enforcement in Bangladesh:**

Bangladesh Bank, the nation's national bank, is cautioning other business banks to be uncertain of individuals utilizing the daddy of digital money. The reason is that, in spite of the huge notoriety appreciated by the virtual cash, the utilization and exchanging of Bitcoin is as yet illicit in Bangladesh. A high-positioning authority of the national bank says that a report managing digital currencies will before long be sent to the Service of Home Undertakings. Meanwhile, the utilization of virtual monetary forms is being observed by the Outside Trade Police Division and other government agencies. The administration of Bangladesh is cautioning individuals not to make exchanges with Bitcoin, and the national bank says that the virtual money isn't legitimate delicate anyplace on the planet. Be that as it may, such isn't the situation as Japan has perceived Bitcoin as a lawful methods for exchange.

At the present time, the fundamental implementation against Bitcoin clients originates from the Bangladesh Budgetary Insight Unit (BFIU). The Remote Trade Police Division, BFIU, and BTRC have officially held four gatherings on chasing down those utilizing cryptographic money.

An authority with the BFIU states: "Banks and other budgetary associations of the nation have been requested to keep up a strict vigil on cryptographic money exchanging. A roundabout will before long be conveyed itemizing the matter. There is no real way to buy these monetary standards lawfully through managing an account channels. Cybercrime specialists are dealing with the issue".

Talking about cybercrime specialists, Nazmul Islam, the Associate Agent Official of the cyber-crime Unit, says: "We have effectively found a couple bitcoin clients, and are on the chase for additional, alongside a couple of site pages which are being checked for credibility. Examining digital money exchanging is a mind boggling matter".<sup>14</sup>

### **5.3 Blockchain mechanism:**

To record digital currency transactions, Block chain innovation empowers disseminated open records that hold changeless information in a protected and scrambled way and guarantee that exchanges can never be adjusted. While Bitcoin and different digital forms of money are the most well-known instances of block chain use, this "circulated record innovation" (DLT) is finding a wide scope of employments. Information stockpiling, money related exchanges, land, resource the executives and a lot more uses are being investigated.

### **5.4 Legalization by various countries:**

The distributed computerized cash Bitcoin made its introduction in 2009 and with it introduced another time of digital money. While impose specialists, requirement offices and controllers worldwide are as yet discussing accepted procedures, one appropriate inquiry: is Bitcoin lawful or unlawful? The appropriate response – it relies upon the area and action of the user. Bitcoins are not issued, embraced, or directed by any national bank. Rather, they are made through a PC created process known as mining. Notwithstanding being a digital currency random to any administration, Bitcoin is a distributed installment framework since it doesn't exist in a physical shape. Accordingly, it offers an advantageous method to direct cross-fringe exchanges with no swapping scale expenses. It additionally enables clients to stay unknown. Shoppers have more noteworthy capacity to buy merchandise and ventures with Bitcoin straightforwardly at online retailers, haul money out of Bitcoin ATMs and use Bitcoin at some physical stores. The cash is being exchanged on trades, and virtual money related endeavors and ICOs draw enthusiasm from over the venture range. While Bitcoin shows up at look to be an entrenched virtual cash framework, there are still no uniform worldwide laws that direct Bitcoin. The Joined States has taken a by and large positive position toward Bitcoin, however a few government organizations work to forestall or diminish Bitcoin use for illicit exchanges.<sup>14</sup> Conspicuous organizations like Dish System (DISH), the Microsoft Store, sandwich retailer Tram and Overstock.com (OSTK) welcome installment in Bitcoin. The computerized money has likewise advanced toward the U.S. subsidiaries markets, which talks about its undeniably genuine presence. The U.S. Division of Treasury's Monetary Violations Authorization System has been issuing direction on Bitcoin since 2013. The Treasury has characterized Bitcoin not as cash, but rather as a cash administrations business (MSB). This spots it under the Bank Mystery Act which requires trades and installment processors to hold fast to specific obligations like revealing, enlistment, and record keeping. Moreover, Bitcoin is sorted as property for tax collection purposes by the Inward Income Administration

---

<sup>14</sup> <https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp>



(IRS). Like its southern neighbor the United States, Canada keeps up a by and large Bitcoin-accommodating position while additionally guaranteeing the digital currency isn't utilized for illegal tax avoidance. Bitcoin is seen as a ware by the Canada Income Office (CRA). This implies Bitcoin exchanges are seen as deal exchanges, and the salary created is considered as business pay. The tax assessment likewise depends whether the individual has a purchasing moving business or is just worried about investing. Canada considers Bitcoin trades to be cash benefit organizations. This brings them under the domain of the counter tax evasion (AML) laws. Bitcoin trades need to enroll with Budgetary Exchanges and Reports Investigation Center (FINTRAC), report any suspicious exchanges, submit to the consistence designs, and even keep certain records. Furthermore, some significant Canadian banks have restricted the utilization of their credit or check cards for Bitcoin transactions. Australia considers Bitcoin a cash like some other and enables substances to exchange, mine, or purchase. The European Association (EU) has pursued advancements in digital money, it has not issued any official choice on lawfulness, acknowledgment or control. Without focal direction, singular EU nations have built up their very own Bitcoin positions. In Finland, the Focal Leading group of Assessments (CBT) has given Bitcoin an esteem included expense excluded status by arranging it as a money related administration. Bitcoin is treated as a product in Finland and not as a cash. The Government Open Administration Fund of Belgium has likewise made Bitcoin absolved from esteem included duty (Tank). In Cyprus, Bitcoin are not controlled or directed either. The Budgetary Direct Specialist (FCA) in the Assembled Kingdom (U.K.) has an ace Bitcoin position and needs the administrative condition to be strong of the computerized cash. Bitcoin is under sure duty controls in the U.K. The National Income Organization (NRA) of Bulgaria has additionally brought Bitcoin under its current expense laws. Germany is available to Bitcoin; it is viewed as legitimate yet exhausted diversely relying on whether the experts are managing trades, diggers, undertakings or clients.

## **Chapter-6-Conclusion**

Avoidance is in every case superior to fix. Digital wrongdoing is expanding step by step. Subsequently we can be a casualty of any digital assault whenever. We should accept careful steps and also correctional measures against cybercrime. To make it productive, the Assembly, the Service of Data Innovation alongside the IT experts and the media must cooperate. The youthful age must be cognizant about cybercrime. Aside from checking and controlling cybercrimes, Bangladesh PC Security Occurrence Reaction Group (BD-CSIRT) should take correctional measures against the wrongdoers and at times BDCSIRT should make a move specifically against the individuals who take part in doing unsafe exercises against understudies, society, state, political and religious convictions utilizing telephone, PC and other guarantee gadgets. The Advanced Security Act, 2016 reinforces the hand of Bangladesh-CERT to make crisis move against digital criminal exercises. Other than National Computerized Security Office (NDSA), National Advanced Security Gathering (NDSC)'s development, territorial and global activities make us idealistic as the Bangladesh the internet a protected zone of correspondence in the coming days. Repeat of such occurrences will influence the economy. Shielding budgetary divisions from future digital violations is of most noteworthy worry right now. Given the rising events of cybercrimes in Bangladesh, there is basic necessity for updating the country's financial basis offering organizations over the electronic system. This episodes induced the Bangladesh Bank prescribing to all Banks and monetary foundations to guarantee digital security administration.

- Taking measures for learning existing specialized whole evaluation and helplessness through an exhaustive digital security hazard think about.
- Treating digital security as an aggregate obligation by every money related organization.

- Introducing Against skimming gadgets to the ATM stalls.
- Use of EMV (Euro pay, MasterCard and Visa) Standard card to abstain from skimming.

Such measures were suggested by the Bangladesh Bank on the grounds that such digital assaults were viewed as being fit for causing money related misfortune and making a reputational hazard. They ought to likewise accentuate on:

- Give IT related preparing to aptitude improvement.
- Observing over the IT related issues.
- Testing peril episode.
- Obligatory reception of IT related safety measure to stay away from such episodes.
- Making client mindfulness.

Moreover, Defensive estimates must be taken in accordance with the legitimate strides in controlling digital wrongdoings. It is in every case better to play it safe while working the Web. A man should remember the accompanying things.

To counteract digital stalking abstain from unveiling any data relating to one. This is tantamount to uncovering your personality to outsiders out in the open place. 2. Continuously abstain from sending any photo online especially to outsiders and talk companion as there have been episodes of abuse of the photos. 3. Continuously utilize most recent and refresh antivirus programming to prepare for infection assaults. 4. Continuously keep back up volumes with the goal that one may not endure information misfortune if there should be an occurrence of infection tainting. 5. Never send your Visa number to any site that isn't anchored to make preparations for cheats. 6. Continuously keep a watch on the site that your kids are getting to keep any sort of badgering or deprivation in kids. 7. It is smarter to utilize a security program that gives authority over the treats and send data back to the destinations as leaving the treats unguarded may demonstrate deadly. 8. Site proprietors should watch movement and check any unpredictable exercises on the site. This might be finished by putting host-put together interruption identification gadgets with respect to servers. 9. Utilization of firewalls might be useful in the security of Digital wrongdoing. 10. Web servers running open locales must be shielded independently from interior corporate system. 11. Programmers hack our own data by utilizing our record ID and secret key, for example, our bank, email ID and secret key. So the most ideal approach to secure us by utilizing exceptionally solid secret key, we ought to never impart our ID and secret word to other individual and never record our secret phrase somewhere else. 12. Before utilizing any PCs please ensure your PC is anchored. We can anchor our PC by utilizing solid firewall programming. Firewall is an extremely solid digital safeguard programming. 13. Utilize hostile to infection programming or projects. Before introducing any projects please ensure this is anchored and confided in site. 14. We ought to introduce the most recent working framework. 15. We ought to never share our own on-line account data with obscure individual.

### **6.1 Recommendations:**

The accompanying advances ought to be taken to anticipate cybercrime in Bangladesh:

1. Clear and plain as day standard working methodology to be forced instantly for the Cybercrime Unit.
2. A thorough enlistment projects ought to be created for every one of the worries of ICT as pilot premise.

3. A different Cybercrime Security Act ought to be instituted.
4. Further there is a critical requirement for developing a code of morals on the internet and order.
5. There must be clear working system for cybercafé and voice over Web convention (VOIP) in Bangladesh. Bangladesh is a nation of sacred matchless quality. Sacred Shield against digital wrongdoings may escort the Digital fighting to a national demeanor.
6. Exceptional prepared wing of police to battle digital wrongdoing ought to be built up. The ascent of digital wrongdoing demands the law implementers to fill in as worldwide police instead of local or national police as it were.
7. Digital wrongdoing units can be set up. Remembering the current circumstance of utilizing Web and expanding digital wrongdoing in Bangladesh, Government can likewise begin such kinds of offices. The centrality of such Units is that these will have the capacity to perform multidimensional activities like propelling the Web foundation, keeping up the ISPs, settling the Web utilizing charges, keeping the digital dangers and so on.
8. Watch Gathering ought to be built up. These gatherings can be one of the imperative constituents for creating Bangladesh as a propelled nation particularly in Web innovation.
9. Open Mindfulness ought to be firmly made. This course isn't less vital than innovative prudent activities. Since more often than not average folks turn into the casualties of digital dangers and a large number of PCs are smashed away. Along these lines, in the event that it is conceivable to mindful the masses about the nature, conceivable hindrance and the fix of the dangers, it would be increasingly advantageous to vanquish digital culprits and additionally spare the virtual world and government can assume the urgent job here.

## **6.2 Conclusion:**

At present we are a creating nation and attempting our best to be a created one. So as to digitalize Bangladesh there is no option to anchored innovative headway among which legitimate web utilizing ought to win in need. This headway requests ICT specialists of which we have extraordinary lacking. The state should push ahead for making such specialists with vital national endeavors. Other than this statutory shields ought to be made best by executing the previously mentioned course of activities. At last, we need to recall that innovation is a wonder such as this which is altering its tendency and course every minute and we need to accomplish the most extreme capacity to battle its adjustment in each minute change both in physical and virtual world for a never-ending presence.

## **References:**

### **Bibliography**

1. Ahmed, Z. (2012) “A Text Book on Cyber Law in Bangladesh”, National Law Book Company, Dhaka.
2. Ahmed. D. Z. (2014) Bangladesher Cyber Ain Totto o Bishleshion (Bangla), Muhit Publications, Dhaka.
3. Kumar Vinod – Winning the Battle against Cyber Crime.
4. Kapoor G.V. - Byte by Byte.
5. Monjur Kader: Criminology (Cyber Crime).
6. The Information and Communication Technology Act, 2006.
7. Duggal Pawan – The Internet: Legal Dimensions.
8. Verton, Dan (2003), Invisible threat of cyber-terrorism.
9. Karzon Sheikh Hafizur Rahman, 2008-Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, pp-411-418.
10. Maruf, M.A, Islam, R, Ahmed, B (2010), Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies, The Northern University Journal of Law, ISSN 22182578, Volume I (2010)

### **SELECTED WEBSITES**

1. <http://bcc.portal.gov.bd>
2. <https://news.bitcoin.com>
3. <https://www.dhakatribune.com/business/banks/2017/12/27/bangladesh-bank-ban-bitcoin/>
4. <https://www.internetsociety.org>
5. <https://www.researchgate.net>