

Cyber warfare Strategies, techniques and tools for Security practitioners.

DISSERTATION SUBMITTED TO DAFFODIL INTERNATIONAL UNIVERSITY IN
PARTIAL FULLFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE
DEGREE OF

MASTER OF LAWS

2019 - 2020

Md.Monirul Alam

ID: 193 – 38 – 348



FACULTY OF HUMANITIES AND SOCIAL SCIENCE

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA 1207

2020

Letter of Acceptance

To

Md. Abu Saleh

Assistant Professor

Department of Law

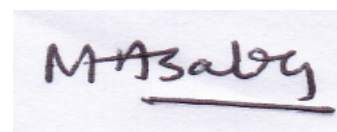
Daffodil International University

Subject: Cyber warfare Strategies, techniques and tools for Security practitioners.

Dear Sir,

It's really a massive gratification for myself to submit a legal research on "Cyber warfare Strategies, techniques and tools for Security practitioners.". My best efforts have been already made to finish my thesis with reasonable collected from a range of sources that I have obtained. I tried my best to uphold the ordinary basic quality at my level.

I, therefore, wish and hope that this research paper will be kindly reviewed for transformation. For any understanding of any portion of this research paper, I will always be open.

A rectangular box containing a handwritten signature in dark ink. The signature appears to be 'M. A. Saleh' with a horizontal line underneath the name.

.....

Signature of the supervisor

Sincerely Yours,

Md. Monirul Alam

ID- 193-38-348

Department Of Law, DIU

Acknowledgment

First of all, I would like to thank my merciful and passionate God for giving me the opportunity to complete my research work. The purpose of this study is to present my subject as clearly and concisely as possible. I have completed my dissertation on “**Cyber warfare Strategies, techniques and tools for Security practitioners**”. This dissertation represents the details of the basic concepts like definition, classification, characteristics, history, legal documents with some case references etc. Cyber Warfare; Strategies, Techniques, and Tools for Safety Practitioners. Inevitably, there may be some inaccuracies in this research case but we have tried our best to include accurate and important data. So, I kindly request please avoid mistakes and consider the only positive aspects of this study.

Dedicated To

My Inspired Idol myFather and Mother

Abstract

The increasing expansion and diversification in the strategies and practices of cybercrime has become a difficult obstacle in order both to understand the extent of embedded risks and to define efficient policies of prevention for corporations, institutions and agencies. The present study represents the most comprehensive review of the origin, typologies and developments of Cybercrime phenomenon over the past decade so far. By means of this detailed study, this paper tackles the issue first describing and discussing former different criteria of classification in the field and secondly, providing a broad list of definitions and an analysis of the cybercrime practices. A conceptual taxonomy of cybercrime is introduced and described. The proposal of a classification criterion is used in conjunction with a cybercrime hierarchy derived from the degrees and scale of vulnerability and targets.

Table of contents

Declaration and Certificate	III
Acknowledge	IV
Chapter – 1	
Introduction	
Background.....	01
Literature Review.....	02
Objective.....	03
Research Questions.....	03
Methodology	03
Significance of this Research.....	04
Chapter – 2	
Techniques on cybercrime	
What is cyber-crime	05
Different types of cyber-crime	06
a) Impact of Cybercrime against Individuals.....	06
b) Impact of Cybercrime against property.....	06
c) Impact of Cybercrime against the Government.....	07
Reasons behind cybercrime	07
a) Ability to store information in relatively little space.....	08
b) Easy to get	08
c) Complex.....	08
d) Carelessness.....	08
e) Loss of proof.....	09
Most Common Types of Cybercrime Law	09
1. Fraud.....	10
2. Data fraud	10
3. Social Engineering	10
4. Software Piracy	10
5. Child Pornography	10
6. Viruses.....	11
7. Cyber Harassment	11
8. Terrorism.....	12
9. Cracking.....	12

Chapter – 3

Cyber-crime in Bangladesh

Use of Internet in awful Intention	15
Bangladesh isn't sheltered from cybercrime	15
Bangladesh is in Danger,.....	16
Bangladesh under a genuine cyber danger	17
Bangladesh PC society site hacked by Libyan programmer.....	17
Current Situation in Bangladesh.....	18
An International viewpoint on cyber-crime.....	18

Chapter – 4

Within Country Strategy

Cyber laws in Bangladesh	19
The Information and Technology Act, 2006.....	19
Digital Security Act 2018.....	22
Cyber law in United Kingdom	25
Cyber law in Republic of India	25
Cyber law in People's Republic of China	25
Cyber law in United States of America	26

Chapter – 5

Some approaches to help ensure yourself against cybercrime

1. Utilize a full-administration web security suite	26
2. Utilize solid passwords	27
3. Keep your software refreshed	28
4. Deal with your social media settings	28
5. Reinforce your home system.....	28
6. Converse with your children about the web	28
7. Stay up with the latest on significant security ruptures	29
8. Take measures to help ensure yourself against wholesale fraud	29
9. Realize that data fraud can happen anyplace.....	29
10. Watch out for the children	29
11. Realize what to do in the event that you turn into a victim	30

Some ways for governments to tighten up cyber security.....

1. Treat cyber security as a basic hierarchical issue	30
---	----

2. Install greater security into your production network	30
3. Empower creative cyber security arrangements	31
4. Team up with the private part	32
5. Plan your ability needs cautiously	32

Chapter – 6

Conclusion.....	35
-----------------	----

Bibliography	36
--------------------	----

Chapter – 1

Introduction:

1. Background of The Study

New correspondence structures and computerized inventions have improved the way we live. The Internet has grown significantly in recent decades. In this day and age, public outsiders are not bound by this kind of crime, which is offensive to the mechanical conditions of the global market. In Bangladesh the rate of web client is expanding quickly. Cyber-crime is spreading in the nation but Bangladesh still does not have any tools to fight this. Cyber-crime envelops any criminal act managing PCs and systems. It additionally includes traditional crimes conducted through the Internet. A number of developing states have introduced or are introducing new laws on cyber-crime, but we have not received any positive efforts from the administration to enforce cyber-laws in our country, regardless of us in Bangladesh.

Despite the fact that Bangladesh is a poor nation, in the light of cell phone network access, the Internet has long been practically accessible to every district in our nation. People begin to identify what the web is and what the cyber world is. We currently have a large number of cyber bistros in our country. Young people are severely addicted to the web and PC.

They want to invest a lot of energy in PC. This is an exceptionally important time for our nation. The Financial express on 10 January 2008 distribute one report expressing that with an inactive cyber law and a serious absence of the skill important to recognize cybercrime Bangladesh has turned into a place of refuge for anybody carrying out a PC crime. As per Net art, a UK organization that is doing exploration and investigation on web applications – Bangladesh has been distinguished as one of the best ten hosts for staging locales for facilitating counterfeit

sites or sending counterfeit messages to get secret data. The web has become an important part of our lives. Bangladesh has a developing region for data development. With the ascent of current innovation Bangladesh like each other country attempting to go on with the expanding speed that is the reason there is a requirement for explicit laws to control cyber-crimes The idea of cyber law is particularly new in Bangladesh. No Bangladeshi essayist yet composes any book on cyber law. There are not many accessible books on cyber law in the market of Bangladesh.

2 Literature Review

This is a study based on, “Combating Cyber Crime in Bangladesh on basis of Laws and Policies”. Many men define the Cybercrime and control, based on their experience. Many people define, “what is cybercrime?” But I think some materials are missing in their research, that is, “Have any specific body to control it? I think their definition is not clear on the basis of this question”. Now a day’s many cases are filled on the basis of cybercrime. Sufi Faruq Ibne Abubakar, only one person; who write on this topic only in his article. He said that, “The concept of a Digital Bangladesh is welcomed by the IT professionals and the general mass. To fuel this notion the government must give due importance to the matter of cybercrime. Otherwise, like many other positive initiatives this will fall on its face. It is a matter of hope that the “National Information and Information Technology Guidelines 2009” has included Cybercrime as an agenda. To make it a success, the Ministry of Information Technology as well as IT professionals and the media must come forward.” In Bangladesh perspective we have a law, based on cybercrime is ICT Act 2006. But this is not sufficient to reduce cybercrime. We have a body that can control it There are many loopholes in our laws. Internet use has become a part and parcel of every educated person in the world. However, it does not agree with him that nowadays there is not only an educated person, but also an

illiterate person involved in the Internet, For that reason, they won't detect which is the harmful web, and doing unlawful activities. But they aren't well known about the proper use of internet. On the other hand some bad people who are educated and some illiterate they voluntarily conduct such illegal activities on the internet. Nowadays anyone can easily enter the internet but if we have an organization to control the field of internet and have some strict rules for internet access then we can reduce the illegal activities in that case.

3 Significance of this Study

To create a safe area for a cyber home, creating a body is very important. Those who have a lot of knowledge about the internet and other such things, which are related to technology. This study is very important to encourage the government to build safety houses. If we only create an agency like the police or any other law enforcement agency to protect this sector and if we maintain a strategy like- "Anyone who wants to access the internet has to maintain a rule, we can easily create Net to trap the criminal. The rule is - each person must register for Internet access by their national identity number or their birth certificate number ", then they can access. Otherwise they don't. This way no one can double-digit ID numbers on any site (such as social media sector, official sector, government sector, etc.). And all access is recorded and stored. Some other rules are also important that after accessing any one of the red marked pages a notification will reach the security house and the agency can easily arrest the culprit and then we can easily apply other laws to prevent cybercrime.

4 Research Questions.

1. How many strategies in cyber crime?
2. What is the current situation of cyber crime in Bangladesh?
3. Viewpoint of cyber laws between Bangladesh and others?

4. What kind of approaches can be initiative against cybercrime?

5 Methodology

This analysis is a qualitative and quantitative basis. I also include the journals, Laws, reports, statistics, and also opinion of many specialists. Firstly, I want to find problems. What kind of problems will occur for internet usage. I want to find out the crimes that are related to the internet. Then I get the laws that deal with this kind of crime. I should seek expert opinion that Whether or not laws are sufficient to fight cybercrime. I also collect this report to learn about crime statistics. I would then like to find out the shortcomings of our laws and address them and describe the process involved in my research. Whenever a particular situation requires a quick assessment because of the urgency of the situation or because of resource or time constraints, professionals make a rapid assessment of that situation by using appropriate methods and techniques. Determining the correct method of any rapid assessment depends on the nature of the situation. So a special method had to be created to make an assessment of the **Cyber warfare Strategies, techniques and tools of safety practitioners** is an emotive and complex.

6 Objectives:

The main object of this research is:-

- Creating a secure home in the cyber sector
- To make a friendly environment
- To prevent crime
- To give a crimeless digitalization country
- To protect youth generation and society

Chapter – 2

Techniques on cybercrime

What is cyber-crime:-

Cyber-crime is a term for any illegal activity that is used as a necessary procedure for a PC commission. In the United States, the Department of Justice uses cybercrime as a means of proving any kind of illegal activity. The evolving shift in cybercrime includes crimes that have made PCs predictable, for example, organizing disruptions and scattering of PC infections, such as PC-based existing crimes such as wholesale fraud, stalks, torture and intimidation.

There are various questions surrounding cyber-crime. Assessments contrast, for instance, with respect to whether some far reaching activities, (for example, document sharing) ought to be delegated criminal acts. The U.S. Advanced Media Copyright Act (DMCA) of 1998 stipulates that trading records of copyrighted material, for example, music or recordings, is illicit and deserving of law. In August, 2002, the U.S. Bureau of Justice reported that they would start to indict instances of shared robbery. Since then, sporadic lawsuits have been filed against the people. Such national formats are plentiful in the media yet are still less familiar with the overall population. Gary Shapiro, leader of the Consumer Electronics Association, has commented that "On the off chance that we have 70 million individuals in the United States who are violating the law, we have a major issue."

Another controversy over cybercrime is the impact of computerized surveillance and general freedom. Since the psychological oppressor assaults on the World Trade Center in September 2001, many have esteemed it important to shorten some individual rights to protection of data in return for more prominent security. As indicated by the American Civil Liberties Union (ACLU), government reconnaissance systems screen gigantic volumes of private interchanges and apply man-made brainpower (AI) applications to sift through significant information.

Albeit such broad observation may fundamentally diminish the likelihood of cybercrime, it is about difficult to do as such without encroaching upon individual protection. Besides, in light of the fact that reconnaissance associations work stealthily, they are not open to investigation. The ACLU recommends that while reconnaissance can be viably used to diminish cyber-crime, it must be legitimately supervised to guarantee that it isn't at the expense of individual rights.

Different types of cybercrime: -

Cybercrime can be broadly divided into 3 main categories:

1. Cyber-crimes against people.
2. Cyber-crimes against property.
3. Cyber-crimes against government.

1. Impact of cyber-crime against Individuals:

Cyber-crimes perpetrated against individuals incorporate different crimes like transmission of tyke sex entertainment and provocation through email. Trading, circulating, posting and spreading pornography, including sexual entertainment, is one of the most important cybercrimes of today. Cyber badging is an unintentional cyber-crime. Badgering can be sexual, racial, religious or other. This additionally leads us to other related areas - native violation which is a crime of a serious nature.

2. Impact of Cybercrime against property:

This activity is commonly referred to as hacking. Indian law, however, makes a distinctive promise to the term hacking, so as the term used in the 2000 law is more broad, we will not use the term "hacking" in contrast to the term "unnatural" rather than hacking..

Bangladesh's budget agencies are at risk from programmers. Money companies in the country have offered various online highlights like web-based banking, stock trading transactions but are not ready to offer the most amazing protection.. Source said the cybercriminal organizes

through Internet have assaulted our nation's innovation foundation. Towards the end, the programmers intervened in the DSE transaction, leaving the small business foresight without any doubt.

3. Impact of Cybercrime against the Government:

Cyber psychological warfare is a special kind of crime in this category. The development of the web has proven that the cyberspace vehicle is being used by people and communities to weaken global governments as well as to threaten a nation's indigenous peoples. Cyberbullying can be identified as "the planned use of risky activities or its risks" for the convenience of social, ideological, religious, political or comparative targets or with the expectation of intimidating an individual's progress.

Reasons behind cybercrime:

Hart in his work "The Concept of Law" said that 'people are powerless so principle of law is required to ensure them'. By applying this to the cyberspace we may state that PCs are powerless so guideline of law is required to secure and shield them against cyber-crime. The purposes behind the powerlessness of PCs might be said to be:

1. Ability to store information in relatively little space:-

PCs have a feature of throwing information in a small space. This takes much less consideration than the demand for data access or expulsion through physical or virtual media..

2. Easy to get :-

Experienced problems in protecting a PC structure from being unacceptable have every possibility of being unacceptable not because of human error but because of bizarre inventions of the mind. Secretly embedding a logical bomb, keys, lumberjacks that can get codes, powered voice recorders; Can run retina imagers and some more biometric frameworks, and sidestep firewalls can be used to go beyond numerous security frameworks.

3. Complex-

PCs chip into working frameworks and these functional frameworks thus create lots of lines of code. The personality of man is uncertain and it is beyond the realm of imagination that will probably not pass at any stage. Cybercriminals exploit these secrets and enter PC structures using more refined methods, often more predictable than initially predicted by framework engineers.

4. Carelessness:-

Carelessness is strongly associated with human lead. As a result there is indeed a possibility that there may be some negligence in securing the PC structure, which thus gives a cyber criminal to gain access and authority over the PC structure. This inattention can lead to improved security, which is usually the property of resource-rich IT security systems, and improved security barriers within software bundles and system structures.

5. Loss of proof:-

Loss of evidence is a very regular and obvious problem because every piece of information is regularly deleted. Gathering more information outside the regional degree similarly disables this system of criminal testing.

The most common type of cybercrime laws

Cybercrime Any criminal activity that takes place in cyberspace. Soon and the most known kind of cyber crime activity hacking. It usually started in the 1960s. These include taking personality and critical data, ignoring protection, and submitting fraud to others.

As indicated by the Identity Theft Resource Center, more than 170 million individual records were uncovered through 780 information security ruptures in 2015. The worldwide expense of cybercrime is relied upon to hit \$6 trillion by 2021. 30 to 40% of organizations are influenced by cybercrime. From 2017 to 2021, organizations are relied upon to spend more than \$1 trillion for cybersecurity.

Every nation on the planet has their transferred laws and standards against cybercrime activities. In the United States, they have fun cybercrime laws that prevent wholesale fraud, hacking, hacking into PCs, and child pornography, among others. In the following sections, we will decide on the most well-known recognized types of cybercrime.

1. Fraud

Fraud is a general term used to describe a cybercrime that expects a person to cheat in order to increase the amount of information or data needed. Any data can be altered, destroyed, taken or smoothed for verification outside of illegal or off-line verification

2. Data fraud

Theft is a different type of fraud in which cybercriminals take personal information, including personal passwords, financial balance information, MasterCard , check cards, social security and other sensitive information. Through data fraud, culprits can take cash. As indicated by the U.S. Agency of Justice Statistics (BJS), more than 1.1 million Americans are victimized by wholesale fraud.

3. Social Engineering

Social engineering is a strategy that allows cybercriminals to reach you by telephone call, message or even face to face. Basically, they will also work like a real organization. These will become a close acquaintance with you until you provide the information you need and unique information to gain your trust.

4. Software Piracy

The web has been loaded with down powers and various projects that illegally copy unscientific material, including music, books, movies, collections and software. This is a crime because it means possession of copyright. Due to software piracy, companies and engineers have seen a relentless reduction in their salaries in light of the fact that their items have been illegally replicated.

5. Child Pornography

Child pornography is a growing cyber -crime and is considered a cyber- crime against people. According to Crime Research, child pornography includes the prevalence, transactions, scattering and posting of child pornography. While carrying out this cyber- crime, the guilty parties will post rebellious photographs and recordings of children and minors. This will allow those who agree to accept their sites to pay for free or subscription. Law enforcement agencies are trying to combat this cybercrime by acting as spies on the web, acting as regular children or as individuals interested in surveying or acquiring individual pornography. The FBI has an unusual unit in Maryland called the Innocent Images National Initiative dedicated to the fight against child pornography on the web.

6. Viruses

A significant cyber crime that affects us today are viruses and they are considered cyber crimes against people. Viruses are transmitted to access their own data on another person's PC and in the long run to crash into their hard drive. A standout amongst the most famous and wrecking viruses as of late was the "Melissa Virus." This infection started to taint PCs in March of 1999 and it spread rapidly. As indicated by Crime Research, the Melissa Virus contaminated 1.2 million PCs in the United States and the harm it caused cost in excess of 80 million dollars to fix. To fight the virus, companies and people can buy adverse reactions from infection software for their PC, if they realize that the source is completely sheltered and the message is not open from anyone, they have no idea about the fog.

7. Cyber Harassment

Cyber harassment comes in numerous structures and is considered a cyber crime against people. It can be very good sexual, religious or racial. It could similarly involve abusing someone else's security using the Internet. To combat cyber harassment, people need to report

any alleged cases to their nearest law enforcement agency. Law enforcement offices will take the best possible steps to identify the harasser and forcefully charge them.

8. Terrorism

Terrorism is known to be a cyber crime against the government. This form of cybercrime might involve the use of the Internet to talk to various oppressors based on fear, to exchange funds to finance an act of psychological oppression, or other related behavior. The law enforcement agencies, in particular the FBI, have odd units to fight this form of cybercrime. The FBI has a rare unit that is known as the cyber terrorist branch.

9. Cracking

Cracking involves harming PC source codes, transmitting false computerized marks, hacking, breaking classifications and transmitting obscene or lecherous electronic data, as suggested by Crime Research. It may well be either a cybercrime against citizens or a government. These guilty parties also take data and then plant an infection to decimate the PC. Cracking can be difficult to illuminate, so any speculated cracking crimes should be discussed with a neighborhood law association. The FBI can opt to seek it in the event that they don't have the labor to seek the guilty party.

Chapter – 3

Cyber-crime in Bangladesh

Science and ICT Progression depends on the extension associated with the division of media transmission. This section is immature because, even with open challenge, there is no deregulation. Bangladesh is not troubled by the effects of cyber-crime on the grounds that monetary transactions have never been fully promoted on the internet. As before, online PC crimes are allowed to increase at an impressive pace as long as money-related transactions are detected, even if the government of Costa Rica obtains the instruments and structure to stay away from, distinguish and indict them. Yet, our administration remains unaware of the facts. A few individuals currently send pernicious mail to various remote conciliatory missions in Bangladesh one morning alongside various VIPs, which now and again create difficult problems with the police and also with the administration.

A few months ago, a gathering of people hacked the Rapid-action-brigade in Bangladesh website. Much of the legislature's leadership ended up frightened at the stage where this event was distributed in the media. There's no reason to believe anyone. After that, a few individuals were arrested by the RAB and they are currently in custody. Shahe Mirza, one of the simple RAB web programmers, said that in such illegal activities as hacking of imperative government or private pages, no one could use his acquired PC skills. In the wake of listening to his announcement kit, Bangladesh 's master who handles cybercrimes ends up terrified.

Bangladesh War Crimes Tribunal Chief Stops over Skype outrage: The leader of a Bangladeshi court that handled crimes carried out in the 1971 Bangladesh War of Independence against Pakistan surrendered yesterday in the midst of debate over the break of his Skype conversation with an exiled legal master of Bangladesh.

Md Nizamul Huq, chief of the Worldwide Crimes Tribunal, referred to "individual motives" for his resignation, State Minister for Law and Justice Quamrul Islam revealed yesterday evening to The Daily Star. His abdication will not hamper the council trials set up in 2010 to prosecute the proof bodies for crimes against humanity, said sources concerned.

The Correspondence Technology (ICT) Act covers vast amounts of legal views to arraign cyber crime, but since its sanction it has not been successfully enforced. The underlying reason behind the ineffectiveness of the law, as demonstrated by the master sentiment, is the absence of legal aid and social and open mindfulness regarding computer crimes. Despite the fact that pornography is not seen as illegal worldwide, cyber-crime experts call attention to it, but it is one of the transcendental PC crimes in Bangladesh. Evidence of the existence of illegally facilitated explicit sites with surrounding drugs is now visible. Today , young people in Bangladesh are increasingly using cyber bistros as their dating sites. Different kinds of antisocial practices take place in these bistros for the sake of net perusing, as suggested by paper records. There are independent lodges for sets for Internet streaming, where their personal minutes are furtively videoed.

These pictures will be made available on the Internet later. An person convicted of the movement of foul and indecent material on site is guilty of a 10-year detention and a fine of Tk one crore, as indicated by section 57 of the ICT Act 2006. Be that as it may, nobody cares about it in view of the fact that we have no viable cyber council to tackle this problem in our country despite all. That is the reason why discipline is easy for cyber criminals in Bangladesh to dispose of.

❖ **Use of Internet in awful Intention**

The opposite sides of a coin are there. In essence, the site also has desires and burdens. The Web can be used as a deadly, massive weapon. One country can be obliterated by using web fear mongers. Since it includes a sound account of a March 1 experience between angry armed force officers and the head administrator, the Bangladesh government put a restriction on opening you-tube video platform only a few weeks ago. In the midst of a passionate meeting at the Dhaka cantonment, the account was made on March 1. Several officers were available, distraught after paramilitary soldiers mercilessly murdered more than 50 military personnel, including a large number of Bangladesh Rifles fringe convincing pioneers. In view of a valid concern for national security, the Bangladesh government reports to the media that you-tube has been obstructed.

❖ **Bangladesh isn't sheltered from cyber crime**

Cyber-crime administrative insights are not surprising, but district judges have been hired to prosecute cases with regard to the Reform Code and the Criminal Code. The number of cyber-crimes caught is limited to the risks of emails. Only 0.3 percent of the entire population has PCs and 0.7 percent access the internet, as suggested by an administration analysis led by the Bangladesh Computer Council. In September 2007, the Denial of Service (DoS) attack influenced most network access providers (ISPs) in Bangladesh. A large number of data parcels were transmitted from an American server farm and induced server dissatisfaction, reducing the installation of virtually all ISPs. The attack was initially attempted on a single ISP, Global Access Limited (GAL). Such violence causes real harm. In any event, our administration remains quiet after the attack, saying that we have nothing to do before the media.

❖ Bangladesh is in Danger

Oppressors focused on cyber-fear are masters. It is not possible to be caught by the traditional police. An intricate part of the cutting edge war is cyber warfare, but it's anything but another aspect. It has previously been named by various names-insight and electronic combat. For example, driving a general public to the verge of collapse through a fascinating electronic disruption to banking frameworks or aviation authority structures, a portion of the cyber fighting thoughts are nuts. For potential cyber combat, fanatical gatherings train their specialists. Likewise, progressive associations use the Internet to concentrate on their communities of onlookers without relying on unmistakable instruments such as radio, television, or the news. The police force of our nation has not been established even now. They are not masters like the Department of Inspection of the American Government. That is why perpetrating crime in Bangladesh is incredibly easy for cyber crooks. Despite everything in our country, we don't have any cyber laws either. Some people are actually using Facebook on the site for several days in Bangladesh. Facebook is a networking tool that brings people together. Understudies are visually impaired, face book fanatics. Understudies basically use facial books during the day. They transmit their photographs, they send their message to their companions via this web. In either case, for business purposes, the problem is that a few individuals use Facebook. They share illegal things and advertise them on Facebook. Understudies are welcome to join such a large number of bogus clubs. Some gathering invite understudies network to come and enter Dhaka city's diverse small night club. The group of Understudy individuals is heading towards being influenced by this kind of note. Almost all of the college strictly confined their understudies to open Facebook in the PC lab in the middle of the class time because this platform actually hindered the instruction of the understudies. Such a large amount of crimes were effectively committed via Facebook.

❖ **Bangladesh under a genuine cyber danger**

In 2004, one kid named Partho was blamed for sending a compromising email to previous Bangladesh PM Sheik Hasina for scarcely any years. He was arrested by the police after that. After they find that one kid using cyber bistro PC sent an email to Sheik Hasina and that kid was Shaibal Saha Partho, the review group is supported by the IT master of the CID group. In this case, the police are also helped by the remote master of cyber law. In any event, the problem emerges after the capture on the ground that there is no law available in our nation to tackle this problem is the reason why it turns out to be exceedingly problematic for the police to go for the further procedures and because of this, the police take a varied approach and that is torment that is not supportable. In the midst of the time parcel of individuals, our administration encourages our nation to enact cyber law, but it is not executed today and the administration still remains quiet about the subject.

❖ **Bangladesh PC society site hacked by Libyan programmer**

The hacking took place from 5-8 November after a few days of a 3-day "Local Seminar on Cyber Crime in Dhaka." Australian High-tech Crime Center (AHTCC) Cyber Crime experts went to the course and learned about various Internet crimes. In any event, after a few days of the workshop, the hacking of the website of an important association such as the Bangladesh Computer Society occurred. The association has been working for a long time in Bangladesh to develop information & communication technology. It has worked in the fields of advancing and making people aware of the use of PCs, serving as a communication between PC professionals at home and abroad. Cyber attacks in Bangladesh at the beginning of the success of ICT are disappointing news. Concerned ICT individuals hope that the specialist would make a stern move toward this form of cybercrime redundancy.

Current Situation in Bangladesh:-

The advancement of science and ICT is focused on the creation of the department of media transmission. Because of the absence of deregulation and transparent problems, this division is still nascent. Bangladesh is not troubled by the effects of cyber crime on the grounds that budgetary transactions have not yet been thoroughly promoted on the internet. Online PC crimes can escalate at a phenomenal pace when money-related transactions are allowed, even if the government obtains the equipment and framework to anticipate, discern and indict them. Whatever that may be, our administration is still not aware of the facts. When the protection level is deficient, web administrations provided through the neighborhood are powerless against comparative assaults and programmer interruptions all the more frequently. A few individuals in Bangladesh send malevolent mail to various remote discretionary missions and various VIPs, creating serious problems for the police and even for the administration once in a while.

An International viewpoint on cyber-crime:

Cyber-crime still ends up being real. Discoveries from the 2002 Information Crime and Security Survey indicate an upward trend that demands a timely audit of current ways to cope with the battle against this modern wonder in the data era. We offer an outline of cybercrime in this paper and provide a global point of view on the battle against cybercrime. In different nations, we audit the ebb and flow status of cybercrime combat, which relies on legal, hierarchical and creative methodologies, and recommend four headings for governments, lawmakers, offices of insight and law specifications, and cybercrime combat specialists.

Chapter – 4

Within Country Strategy

Cyber laws in Bangladesh:-

In the midst of the rapid expansion of data and correspondence innovation and broadcast communications organizations in the South Asian country, Bangladesh is organizing stringent steps to tackle cyber crime. The ICT industry in Bangladesh has grown rapidly and is making its success deeply felt in both individuals and private divisions in general. Over five million PCs are currently being used in the nation by industry gauges, with three million site customers. "We have found a way to facilitate the fair and checked use of data innovation because there is no overall law on cyber crime management in the country," says MM Neazuddin, Joint Secretary of the Ministry of Science and ICT. Neazuddin said the government, which has repeatedly promised a "Computerized Bangladesh" in 2021, had supported a fundamental degree of revision of past enactments calling for jail sentences and overwhelming cash-related fines to cope with new forms of crime. The proposed law suggested arrangements for a maximum of 10 years in jail and a penalty of 10 million (US\$ 150, 000) for breaking into PC systems and placing on the web false and slanderous details or revolting content. The legislature would urge the Supreme Court to create at least one cyber tribunal for the expedient and effective indictment of the offenses.

The Information and Technology Act, 2006:

In terms of cyber hunching down, the Bangladesh Penal Code does not have too many arrangements. However, there is nothing found in our corrective code in the event of cyber-crime such as hacking, Internet time burglaries, email bombing. So it can very well be said that by using any structure of the reformatory code, it is not feasible for our administration to monitor cyber crime. It is necessary to enact extraordinary law that only arrangements with cyber-related issues for controlled cyber-crime. In 2006, the Bangladesh government passed

the Information Technology Act. This is the latest legislation passed by the Bangladesh legislature to combine computer-related problems and further arraign PC and PC offense-related arrangements. In terms of damage to the PC and PC system, this resolution involves a few arrangements.

Cybercrime demands that threats or unauthorized access to PCs and PC frameworks are refused. Punishment for messing with PC source archives is given, as indicated by Section 66 of the ICT Act. Section 66 states that whoever purposely pulverizes or changes or purposely or intentionally disguises, demolishes or alters any PC source code used for a PC, PC program, PC system or PC arrangement, will be guilty of detaining either a representation for a period that can exceed three years or a fine that can extend to Taka two lakhs or both.

Hacking with the PC system in section 67. Whoever, with the intention to trigger or know that he is likely to cause unjust misfortune or damage the general population or any other individual, does some act and thus demolishes, erases or changes any data residing in a PC asset or decreases its esteem or usefulness or harms it harmfully using any and all means, submits the hacking offense.

The programmers are disciplined by section 68 of the ICT Act. Section 68 states that for a period that can stretch up to three years or with a fine that can extend to taka two lacs or with both, whoever submits hacking will be rebuffed with detention. Be that as it may, the problem of this act is that a vast number of items are handled by this act. The act is intended to cover all the issues relevant to data innovation. Be that as it may, expecting to cover all of the stuff by merely performing a single act is ridiculous. We need one particular cyber law in our nation to regulate cyber-crime.

By section 68 of the ICT Act, the programmers are disciplined. Section 68 states that anyone who submits hacking will be rebuffed with detention for a period that can last up to three years or with a fine that can extend to taka two lacs or both. Be that as it may, the dilemma with this act is that a large number of things are handled by this act. The act is intended to cover all matters relating to the invention of data. Be that as it may, it is ridiculous to expect to cover all of the stuff by simply performing a single act. To regulate cyber-crime, we need one specific cyber law in our country.

To protect the rights of web associations, the United States, the U.S. Congress has made new laws to direct activities on the web. "The United States has developed numerous cybercrime guidelines with the main computerized signature law on the planet, such as the" National Infrastructure Protection Act of 1996, "the" Cyberspace Electronic Security Act of 1999 "and the" Loyalist Act of 2001. What's more, different agencies have been formed in the U.S. to combat cybercrime, including the FBI, the National Infrastructure Security Center, the National White Collar Center, the Do's Computer Hacking and Intellectual Property Unit, etc. The FBI has developed unusual specialized units and has produced Carnivore. The British parliament has passed two cybercrime-related laws in Britain: the 1984 Data Security Act and the 1990 Computer Abuse Act. The former one provides for the actual processing and use of individual data, while the latter specifies the rules, mechanisms and penalties that require unauthorized access to PCs. The British government has related sifting and ranking advances to protect estates from unseemly web content. The Canadian Parliament passed the Criminal Law Amendment Act, which has two parts, in Canada in 2001. The key section explains the illegal passage of transmissions into a PC system and the capture attempt. The second section condemns the actual decimation, alteration, or intrusion of data. The Kenya Communications (Amendment) Act was passed by the Parliament of Kenya and signed into law on January 2

by the President. In Sections 83 W-Z and 84 A-F, the Act contains the Cybercrime Act on: unapproved access to PC information , access to crime, access to crime,

Unapproved access to and blocking PC administration attempts, unapproved modification of PC content, damage or denial of access to the PC system, unapproved password disclosure, illegal ownership of gadgets and information, electronic theft, messing with source archives of PCs, and dissemination of vulgar data in the electronic structure. "In Norway, a Bill on another Criminal Law (2008-2009) implemented a wholesale fraud agreement in 202, using the word Identity Infringements that peruses as follows:" With a fine or imprisonment not exceeding 2 years, someone who is disregarded would be disregarded, who without authority has a method for someone else's personality, or behaves with the character of another or with a character that could effectively be unapproved access to and block attempt of PC administration, unapproved alteration of PC material, harming or denying access to PC framework, unapproved divulgence of passwords, unlawful ownership of gadgets and information, electronic fraud, messing with PC source archives, and distributing of vulgar data in electronic structure. In Norway a Bill on another Criminal Law (2008-2009) has in 202 presented an arrangement on wholesale fraud, utilizing the term Identity Infringements that peruses as pursues: "With a fine or detainment not surpassing 2 years will whoever be rebuffed, that without power has of a methods for personality of another, or acts with the character of another or with a character that effectively might be mistaken for the personality of someone else, with the expectation of an acquiring a monetary advantage for oneself or for someone else, or b) making lost property or burden someone else." (Unofficial Translation). The Norwegian Parliament has on May 28 received the New Penal Code, including a few arrangements on cybercrime.

Digital Security Act 2018

The Digital security act, 2018 has been passed by the ICT Department of the Ministry of Telecommunications and it has been placed for office approval. This Act is an revised version of the nation's digital assurance law, which will supersede a portion of the questionable digital security law arrangements, similar to Section 57 of the ICT Act 2006. Several important highlights of the Digital Protection Act, 2016-E-Commerce , E-Transactions are viewed and characterized. The ward of the Act, which covers the two individuals within and past the fringes of Bangladesh, is defined in area 4 of the Act. Section 5 addresses the constitution of an Information Protection Agency to screen and guide the advanced substance, communications mediums to anticipate information misconduct, like mobile phones. The Digital Forensic Lab and the Bangladesh Cyber Emergency Incident Response Team (Bangladesh-CERT) are also present in this section. Area 13 of the Act sets out the powers of the DG of the Digital Security Agency, where the DG can, under additional traditional circumstances (security rupture or national-universal risk), prevent correspondence with any person or specialist organization. The person or specialist organization needs to facilitate the block attempt, observing and unscrambling of the machine or source, all things considered. It notes that the Act describes cybercrimes based on area 15 in the form of hacking, pantomime, violation of security and different forms. Area 15(5) of the draft Act provides that any disdainful remarks, statements, fight or advertisement in electronic media by a person, foundation or remote native, against the war of liberty, or the father of the Bangabandhu Sheik Mujibur Rahman Nation, or any matter resolved by the Court, will add up to an offense under this Act. The offense in this area is defined in Segment 36 of the draft Act as cognizable and non-billable. The Penalty for the offenses under Section 15 (cybercrimes, ads against the Liberation War or Bangabandhu) is defined in Area 16 and ranges from 3 years in prison to life imprisonment or theoretically a fine of 10 million taka. The comparative offense of any person who assists or abets the

commission of any offense under the Act is included in Section 21 and may be liable for comparable discipline. Under the Digital Security Act, the preliminary will be hung on the similar Cyber Tribunal established under the ICT Act 2006; the Tribunal 's tactics will also be comparable, completing the preliminary within 180 days.

I specifically clarify that Section 2 of the 2016 Digital Security Act defines what is legitimate access, unlawful access, foundation of basic data, e-exchange, e-installment, defilement of information, information, software, advanced system, endorser data, traffic data, electronic fraud, computerized erotic entertainment, advanced tyke sex entertainment, etc. In either case, the opportunity to represent and chronicle the archives in other fields. How it is stockpiled is not referenced in this Act, in any case. Here, 30 percent of the laws are new, yet 70 percent are redundant with various laws such as the ICT Act, the Penal Code and the Criminal Procedure Code. Obviously, this Act does not characterize where the officer is chosen to maintain the division. Here also some insufficient with regard to the fact that the Police also go about as well this segment and explore it but I think here the IT segment pro should select to manage this region as a law authorization organization.

1. Cyber law in United Kingdom

The Police and Justice Act 2006 Chapter 48 proclaims the corrections of the Computer Misuse Act 1990, Part 5 sections 35 to 38. The new alterations came into power on October 1, 2008.

2. Cyber law in Republic of India

The Indian Government has in 2003 reported plans on a thorough law for cybercrimes.⁶⁶Hacking with PC framework.

(i) Whoever hacked with the intention of causing or discovering that he is likely to cause unfair misfortune or damage to general society or any person crushes or deletes or alters any

data residing in a PC asset or diminishes its esteem or usefulness or affects it harmfully using any and all means.

(ii) Whoever commits hacking will be rebuffed with detainment as long as three years, or with fine which may stretch out up to two lac rupees, or with both.

3. Cyber law in People's Republic of China

Many cybercrime problems in China are veiled in laws and guidelines that allude to Internet-related crimes. The Public Security Bureau (PSB), responsible for interior security, and the Ministry of State Security (MSS), which manages external security, are the two most powerful associations in charge of internal and external security. The functions of the Public Security Bureau (PSB) are officially classified in the Regulations of the PC Information Network and Internet Security, Safety and Management, affirmed by the State Council on 11 December 1997 and distributed on 30 December 1997. Article 285 states that someone who disregards state guidelines and barges through PC systems through agreements relating to state issues, guard office creation, and advanced science and innovation is sentenced to no more than three years of fixed-term imprisonment or criminal confinement. Article 286 states that whoever violates state guidelines and erases changes, promotions and impedance in PC data structures, causing irregular structures tasks and severe consequences, shall be sentenced to no more than five years of fixed-term detention or criminal confinement; if the consequences are exceptionally genuine, the punishment shall be fixed-term detention for at least five years. The previous passage should be rebuffed by anybody who disregards state guidelines and deletes, modifies, or includes the information or application programs implemented in or prepared and distributed by the PC systems, and causes serious consequences. The key passage is to be rebuffed by someone who deliberately produces and proliferates PC infection and numerous projects that damage the standard task of the PC system and trigger serious effects. Article 287

states that whoever uses a PC for money-related fraud , theft, debasement, misappropriation of open properties, taking into account state insider evidence, or various offenses, is to be convicted and rebuffed by the law's relevant laws.

4. Cyber law in United States of America

The National Security and Homeland Security Advisors were coordinated by President Barack Obama to conduct a review of the arrangements, programs , and activities in progress during the cyber security administration, including new recommendations to fight cybercrime. On February 7, 2010, at the 45th Munich Conference on Security Policy, US Vice President Joe Biden gave an introduction. He discussed the need to deal with terrorism and cyber security, among several others.

Chapter – 5

Some approaches to help ensure yourself against cybercrime

In 2018, cybercrime was an evolving threat. You may feel that programmers taking your money-related data are the main form of cybercrime you need to worry about. It may not be so simple, however. There are certainly a wider number of problems than just important money-related ones. Cybercrime continues to evolve, with new dangers emerging every year. You can be tempted to avoid using the web entirely when you hear and learn about the scope of cybercrimes out there. That is most possibly excessively rare. Rather, knowing how to interpret cybercrime is a wise thinking, which can simply be the initial step to safeguarding your information. Evading future danger and understanding who to contact when you see someone online engaging in illegal activity are both valuable advances. You'll need to work out how cybercrime can be stopped, but remember this: you can't. Nevertheless, to help defend against it, you should avoid potential harm.

1. Utilize a full-administration web security suite

Norton Security, for example, offers continuous assurance against current and emerging malware, including ransomware and viruses, and when you go on the web, guarantees your personal and budgetary details.

2. Utilize solid passwords

Try not to rehash your passwords and regularly update your passwords for different destinations. Complexize them. That means using anything like 10 letters, numbers, and images in a mixture. A hidden program for key administration will help you keep your passwords safe.

3. Keep your software refreshed

With your working frameworks and web security tools, this is particularly imperative. In order to enter your framework, cybercriminals usually use documented adventures or imperfections

in your program. Fixing these efforts and imperfections will make it more unpredictable that you will end up a target for cybercrime.

4. Deal with your social media settings

Keep your own and private information secure. Cybercriminals in social engineering can also get your own data with just a few focus points of information, so the less you share publicly, the better. For instance, on the off chance that you post the name of your pet or uncover the original last name of your mom, you can open the answers to two standard security questions.

5. Reinforce your home system

Starting with a solid encryption secret phrase as a virtual private system is a wise idea. All traffic leaving your gadgets will be encoded by a VPN before it touches base at its target. In the off chance that cybercriminals find out how to hack your line of communication, besides encoded information, they will not block anything. Using a VPN at any stage you organize an open Wi-Fi is a good idea, regardless of whether it's in a library, bistro, inn, or air terminal.

6. Converse with your children about the web

Starting with a solid encryption secret phrase as a virtual private system is a wise idea. All traffic leaving your gadgets will be encoded by a VPN before it touches base at its target. In the off chance that cybercriminals find out how to hack your line of communication, besides encoded information, they will not block anything. Using a VPN at any stage you organize an open Wi-Fi is a good idea, regardless of whether it's in a library, bistro, inn, or air terminal.

7. Stay up with the latest on significant security ruptures

In the event that you work with a shipper or have a record on a site that has been impacted by a security break, discover what data the programmers got to and change your secret word right away.

8. Take measures to help ensure yourself against wholesale fraud

Wholesale fraud occurs when someone wrongly gets their own data in a manner that requires fraud or trickery, usually for financial addition. What? How? For example, you may be tricked into giving person data over the web, or a cheat may take your email to get data into account. That is the reason why protecting your own information is important. A VPN, short for virtual private system, can also ensure that you submit and get information on the web, particularly when you access the web on open Wi-Fi.

9. Realize that data fraud can happen anyplace

In terms of travelling, it is shrewd to know how to protect your character. You can do a lot of things to help protect hoodlums from getting your private details out and about. This involve keeping your sightseeing plans away from social media and using a VPN when accessing the web through the Wi-Fi system of your inn.

10. Watch out for the children

You will also need to help defend them from wholesale fraud, just the same as you will need to talk about the web with your kids. Character cheats regularly target children on the grounds that a new start always speaks to their Social Security number and records as a customer. By being watchful when sharing your child's close to home data, you can help make plans for wholesale fraud. It is also keen to know what to look for that could suggest that the integrity of your child has been compromised.

11. Realize what to do in the event that you turn into a victim

You must caution the local police and, now and then, the FBI and the Federal Trade Commission, on the off chance that you trust that you have been a victim of cybercrime. Regardless of whether the offense seems to be trivial, this is imperative. Your study may assist experts in their examinations or may subsequently defeat lawbreakers from manipulating other citizens. In the event that you believe your character was stolen by cybercriminals. These are among the approaches that you should consider.

- >Contact the organizations and banks where you realize fraud happened.
- >Spot fraud alarms and get your credit reports.
- >Report data fraud to the FTC.

Some ways for governments to tighten up cyber security

1. Treat cyber security as a basic hierarchical issue

Advanced protection is not just something that you should leave to the experts in IT. It influences everybody working in government. Pioneers champion preparation and commitment to cyber security in the best models from the private side, and present the risks, all things considered, words, with the aim that everyone knows what is in question and how it impacts their day-to-day work.

Take the oil and gas market, where individual security has been the principal for some time. Organizations in this division have attempted to make cyber security a similarly oriented part of their lifestyle, not just a 'consistency' problem, near to well-being. Staff are encouraged to know what kinds of advantages are at risk and how attacks can be avoided and hazards can be

detected. Governments need to follow a common outlook and make cyber security part of the way we do things around here.

2. Install greater security into your production network

A large and complex snare of specialist co-ops and contractors is often vigorously subordinated to the current governments. With such a large number of gatherings handling private data, the odds for holes or burglary are a lot higher. By taking care of acquisition, the most appropriate solution to countering this test is. Contracts should integrate cyber protection. Providers should all be promised to an industry standard in a perfect world. Customary observation and unbiased feedback will promise the government that values are being upheld in order to stay away from powerless links in the chain. In particular, when responding to a cyber security episode, ensuring contracts drive the right procedures, ensuring receptivity, simplicity and a willingness to comply when the most noticeably awful happens.

3. Empower creative cyber security arrangements

They must still hold one stage in front of hoodlums in the event that administrations need to recognize the reserve funds and efficiencies from going computerized. Packs are cunning and fast; they work to find another when one path becomes blocked. In order to collect innovative and realistic approaches to square cybercrime, governments must be considerably more agile and disappoint the criminals' attempts to money out and adapt stolen data. New technologies, such as biometrics, inspection and virtualization, may have an impact, but instruction and mindfulness can do so.

Lamentably, numerous open part advanced crime aversion ventures turn out to be expansive, costly endeavors that don't generally convey.

In the event that governments need to remember the reserve funds and efficiencies by going computerized, they must always keep one stage in front of hoodlums. Packs are cunning and fast; when one route becomes blocked, they work to find another. Governments must be considerably more flexible in order to gather creative and practical methods to square cybercrime and disappoint the attempts of hackers to money out and adapt stolen data. New technology may have an impact, such as biometrics, inspection and virtualization, but guidance and understanding may do so.

4. Team up with the private part

Given the performance of numerous companies in the battle against cybercrime, a portion of this capacity and expertise should be addressed by the government. Cooperation, such as giving assessments, benchmarking and peer exams, can get fresh, outside reasoning. We put our customers together to provide secure spaces for discussion, share war tales, and find strength in the understanding of each other. The I-4 meeting framework worldwide is just one instance of our work here. It is equally important to be set up to exchange information about real and future assaults. All things considered, the kind of information drifting through the criminal clique is mostly stolen from and used against a combination of transparent and private connections, so cooperating is to everyone's greatest benefit.

5. Plan your ability needs cautiously

Cybercrime is a growing wonder, and it is of immense importance to individuals with the ability to combat this danger. Current governments do not compete with the pay scales of the private segment, so it is difficult to hold on to the best ability. Workforce structures should expect experts to stay for a few years and aim to build a line of young, youthful capacity to replace them.

Governments should extend their cooperative efforts with privately owned companies in the future to integrate capacity sharing. As a major aspect of their characteristic vocation enhancement, cybersecurity professionals could transform jobs between the general public and private areas. It would not simply help the government; it would also offer a higher individual profile to these people.

With respect to physical protection, we are all aware of suspicious conduct. Government officials should all consider themselves at the cutting edge of distinguishing and responding to cybercrime in the future.

Chapter – 6

Conclusion

Cybercrime or cyber issues are as contagious as the data framework around us. In the case of a notice case or relevant analysis, indiscriminate hacking or cybercrime is a crime where straightwary bytes are moving much faster than shots. In order to prevent cyber issues or to hack the planet, all countries need to enact some important and cruel laws by which cyber crimes can be avoided. In addition, all illegal sites that are not approved by the legislatures of countries must be shut down. It is the most imported part of every legislature to provide an educational program on cyber issues or cyber-crime, which is further considered as an additional necessary test to keep cyber issue or cyber-crime all over the world. is likewise required so as to distinguish cyber offenders. Presently multi day's part of web master is accessible in Bangladesh who has got parcel of thought regarding web and cyber world At present all the major private banks in our nation started web-based banking earlier. This web based banking relies on internet and pc. So it is the responsibility of the administration to protect everyone in the bank. There is also a serious need to enact a cyber-crime law that will ensure cyber security in Bangladesh. Cyber police are forced. Only the preparation of the administration is enough to do this. One year ago, the enemies of cybercrime activities were being eliminated in preparation for the experts to come together and create software. Similarly the limitations of cybercrime laws and approvals building and educational classes require further initiatives across all countries.

Bibliography

Books

1. Narayan, P. *Intellectual Property law, (India: Eastern Law Publishing Co. Pvt. Ltd,2001)*
2. Ahmed DR. Zulfiquar, *A Text Book On Cyber Law in Bangladesh*
3. D Rodney Ryder, *Guide to Cyber Laws, 2nded.* (Nagpur:Wadha & Company, 2005)

List of Statutes

1. *The Information Technology Act, 2006*
2. *Digital Security Act 2018*
3. *Penal Code 1860*
4. *Bangladesh Telecommunication Act 2001*
5. *Criminal Code of Procedure 1898*
6. *Pornography Act 2012*

Journals

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

Websites

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