**Abstract**

Cyber crime is known to all over the world as a crime committed through internet. It is, nowadays, becoming a serious matter of concern all over the world. This paper describes the nature of cyber crime which is committed in Bangladesh. As the use of internet in Bangladesh is not as wide as other developed countries, crime, however, related to internet is in emerging stage herein this country. The study is exploratory in nature. Methodological triangulation (face to face interview and case study) has been applied to collect pertinent data from 30 purposively selected respondents. It is revealed from the study that, though cyber crime is not in serious condition in research area, the respondents are victimized sometime by hacker, pornography sites and computer virus through internet. It is continuously growing attention of the majority people of the study area.

Keywords: crime, cyber crime, internet, computer hacking, pornography, identity loss, hacking, computer virus

**INTRODUCTION**

In 1969, the first message, “login”, was sent over ARPANET, the predecessor of today’s internet (Kleinrock, 2008). ARPANET was designed as a communication system that would allow researchers to access information from other researcher’s computers around the country, therefore allowing information to flow more freely. From this humble beginning the internet has expanded far beyond the expectations of the individuals who created it. According to Kleirock, one of chief scientists on the ARPANET, “What I clearly missed was the fact that my 99-year-old mother (now deceased) would be on the Internet; that is, I did not foresee the powerful community side of the Internet and its impact on every aspect of our society”. Computers and the internet have become intertwined into our daily lives.

One reason why individuals use the internet is because they can gather and share information with other individuals no matter where on the globe they are located. This advancement in the way individuals can communicate with one another, as well as the decreasing cost and size of computers, are some of the reasons why internet use has grown so rapidly. Today, the top three websites Google, Microsoft, and Facebook each have over 500 million unique users. The internet allows individuals to easily find information, stay in touch with others, and has even resulted in new ways to conduct business. People’s use of the internet and computers continues to grow as more and more people have access to this technology. However, while this new technology has brought with it much advancement which makes our lives easier, it has also led to advancements in crime.

Internet is becoming popular day by day because of its some special features. A revolutionary change has come in communication and socio-economic transaction by internet. Being facilitated with the virtue of it, people can communicate very easily national as well as international level. Generally it is called on-line communication. It is the vast source of information. We can get any information from the Internet. Though it is the easiest way of communication, now it is the matter of concern that misuse of computer and internet put together some people to commit crime. According to Council of Europe “Any criminal offence committed against or with the help of a computer network is identified as cyber crime” (Council of Europe Convention on Cybercrime 2001:8). So computer is must for cybercrime. Generally Among the numerous crimes in today’s society; cybercrime has become very common as well as very dangerous. The emergence of new technology has increased the number of perpetrators that take advantage of these resources to use them illegally for their own gain (Gjata 2007:5). The most dangerous aspect of cybercrime is that the victims fail to acknowledge the cause of their unfortunate fate. Not only should victims report any sort of suspicion and/or crime, but the victim needs to identify the suspected machine so police can confiscate it in order to have evidence gathered form the machine’s hard drive. Without having the computer form which the perpetrator committed his crime(s) then it is very hard to convict and persecute these perpetrators. Victims of cybercrime need to become aware of such crimes and they need to become more educated in how to protect and prevent not only themselves but others as well from such malicious acts. With today’s advanced technology the urgent need of information security, ethical education and awareness programs cannot be emphasize enough in order to achieve the maximum protection from the hackers and also to protect Cyber world from our own abusive use (Gjata, cybercrime 2007: 7) Numerous government agencies around the world have taken necessary precautions to detect and persecute perpetrators of cybercrime. Although, because of the vast amount of new technology being produces regularly government agencies have to stay alert and informed in order to control cybercrime. Cybercrime can be victimless, but it can also harm unfortunate individuals.

Cybercrime is a worldwide problem now; no country is immune (El-Guindy 2008: 16). The first cybercrimes occurred in India, Japan and china in 1820(Techno focus cybercrime-A looming threat 2008). After that it was increasing evolutionary and at mid of 20th century it became a problem of concern. Around the world and in Middle East and third world countries the growth of Internet connectivity in recent years is significant and simultaneously similar increase in cybercriminal activities (El-Guindy 2008:16). We see in 2001 approximately 28.5 million people in the UK use the Internet (Fafinski 2008:1). Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007(El-Guindy 2008:3). 50% adult use Internet in Australia (Australian federal police: 4). In Bangladesh Internet was first introduced in 1996(Hossain 2004:6). Foskett said Internet users are growing rapidly in Bangladesh especially in the metropolitan areas. In 2000, the number of Internet users was 100,000 and it shot up to 450,000 in 2007.

In another report says about 2 million people use internet in Bangladesh (Hossain 2004:6) In Canada by the year 2000 the 45,950 computer crimes reported by the NIBRS2 and noted that most common type of computer crime was larceny/theft (Kowalski 2002:12). By the years cybercrimes develop besides technical development and by time it created new dimension of crime such as from telecommunication crime to electronic money laundering (Graycar 2000). Because of cybercrime people lost their money, identity and many more.

In the UK there were 92000 cases of on-line identity fraud during 2006 because of that average value of loss from 183.2 to 212.6 million pounds by card-not-present (CNP) fraud. 218.817 incidents of physical harassment were recorded. In 2006 850000 cases of unwanted online sexual approaches occurred (Fafinski 2008:8-14). 38% Drug Importation cases, 34% Defraud the commonwealth cases, 25% Child Sex related cases, 3% Counterfeit currency/documents cases, 45% E-Crime, 11% Interpol, 2% Counter terrorism, 42% Others (Fraud, Credit Card, Money Laundering) occurred in Australia during 2005 and 2006 (Australian federal police: 4-5). The systems of NASA, US Army, Navy and Department of Defense were hacked right after the 9/11 attacks (www.crime-research.org/news/13.01.2009/3692/). Spam is now a great problem in cyber world everyday thousands of Spam spreading through e-mail and other way. Nearly 200 billion Spam messages are now sent each day, double the volume in 2007 — and that targeted attacks are also rising sharply and 90 percent of all e-mails sent worldwide are Spam, this means 800 million messages a day are attempts are spear phishing (www.crime-research.org/latest news/18.12.2008/3681/). One in four (23%) of UK internet users had been victim of phishing scams during the last 12 months, compared to just eight per cent the year before. Similarly, more than one in six (16%) had fallen victim to other types of online scam.

One of the most important issues is child pornography. Because of the Internet pornography industries generate approximately 3 billion US dollars annually and there are roughly100000 websites offering illegal child pornography (Young 2008:287). In Tahlequah Michael Ray Wright had pictures of under aged girls during April 1 & Dec 18, 2008 (www.crime -research.org/latest news/14.01.2009/3693/). Australian Broadcasting Authority found 54% credit card number theft, 45% personal data misuse, 39% privacy issues and 21% incidents because of viruses (Barbara 2002: 4). On the top of the list of cybercrimes registered in 2006 there are 1.94 million cases of harassment, this figures includes e-mails with threatening or abusive statements and offensive allegations left on websites and about 850,000sex crimes including cyber stalking occurred in Britain ([www.infoniac.com/hi-tech.htm](http://www.infoniac.com/hi-tech.htm)). 

Considering the contemporary and early history it is found, 1st world countries are most affected because they were reported but we have no chronological data about cybercrime in our country. The impact of cyber crime is not as alarming in Bangladesh because financial transactions have not yet been fully facilitated online, said Freddy Tan, chief security advisor of Microsoft Southeast Asia. He warned that, as soon as financial transactions are allowed, online computer crimes would increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them. ‘Online financial scams are a major threat for banks, credit card holders and alike.’ ‘Internet services provided through the local area network are vulnerable to similar attacks and intrusions by hackers more often when security level was inadequate. According to a government study conducted by the Bangladesh computer council, only 0.3 % of the total population own computers and 0.7% have access to the Internet. The government statistics for cybercrime are not remarkable, but district judge have been empowered to try cases in reference to the panel code of criminal procedure. The limited number of cybercrime apprehended is confined to e-mail threat (Hammadi 2008: 2-4). An example is that E-mail threatening to such organization and renowned person in Bangladesh (Borhan Uddin 2006: 14). Bangladesh government has launched the initiative of making digital Bangladesh. But the use of internet is limited in this country. People mainly use internet for their educational purpose. Bangladesh is a safe haven for anyone committing a computer crime. From viruses (which infect computers to malfunction), Trojans (deceptive software or malware that appears to perform an action but instead performs another) and Spam to online threats, piracy, hacking (accounts), theft (of data or pin numbers) and pornography, all these facts of computer crime have advanced significantly beyond existing modes of detection So there is no doubt that how important matter that is for the contemporary situations in Bangladesh at the rising time of Internet technology.

**A REVIEW OF CYBERCRIME**

Before examining different criminological theories that have been applied to the study of cybercrime it is helpful to better understand cybercrime. It is useful to understand what type of legislation has been passed to help define what cybercrime is and under whose jurisdiction a cybercrime falls. This information helps us gain a better understanding of cybercrime and the categories of crimes that fall under the label of cybercrime. Along with examining cybercrime legislation, it is also important to study the entities that enforce and combat this problem. Understanding cyber law enforcement gives insight into how the problem is being addressed and thus a better understanding of the problem. Finally, it is important to have an idea of the true extent of the problem by examining the levels of cybercrime among businesses and individuals. This information will demonstrate the need for research into this growing problem. 

**Cyber Crime Defined**

It is a technological crime and a misnomer term. It is also known as computer crime, electronic crime, hi-tech crime and e-crime. Actually it involves a broad range of potentially illegal activities conducted by the misuse of computers and different types of communication networks. Additionally, cyber crime also includes traditional crimes conducted through the internet. For example: hate crimes, telemarketing and internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the internet. Cyber crime is mostly a property related crime. It has no direct contact with the victims and involves less visible and intangible kinds of property such as information, data and computer networks. Victims come to know about their losses long after the actual commission of crimes. Profits from high-tech crimes are vast. Hackers are able to steal greater amounts with greater comfort; a single act can victimize many people in many places at once.

It may be divided into two types:

1. Crimes that target computer networks or resources directly

2. Crimes facilitated by computer networks or devices

Examples of crimes that primarily target computer networks or devices would include malware and malicious code, denial-of-service attacks and computing viruses. Examples of crimes that merely use computer networks or devices would include, among others, cyber stalking, fraud and identity theft and information warfare. It is further subdivided into the following four categories:

 Cyber crime against individuals

 Cyber crime against property

 Cyber crime against organization and

 Cyber crime against society at large

This crime can be broadly defined as criminal activities using information and communication technology including the followings, which can be commuted against the above mentioned groups:

**Against Individuals:-**

a) Hacking or Cracking

b) Illegal/Unauthorized access

c) Illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system)

d) Data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data)

e) E-mail spoofing

f) Spamming

g) Cheating and Fraud

h) Harassment and Cyber stalking

i) In decedent exposure

j) Defamation

k) Drug trafficking

l) Transmitting virus and worms

m) Intellectual property crimes

n) Computer and network resources vandalism

o) Internet time and information thefts

p) Forgery

q) Denial of services

r) Dissemination of obscene material

**Against Property:-**

a) Credit card fund

b) Intellectual property crimes

c) Internet time theft

**Against Organizations:-**

a) Unauthorized control/access over the network resources and websites

b) Exposing indecent/obscene materials over the web pages

c) Virus attack

d) E-mail bombing

e) Salami attack

f) Logic bomb

g) Trojan horse

h) Data diddling

i) Blocking from access

j) Theft of important possessions

k) Terrorism against government organizations

l) Vandalizing the infrastructure of the network

**Against Society:-**

1. Forgery

b) Online gambling

c) Trafficking

d) Pornography (especially child pornography)

e) Financial crimes

f) Polluting the youth through indecent exposure

g) Web jacking

**The crimes mentioned above may be defined briefly as follows:**

**Software Piracy:**

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

**IRC Crime:**

Internet Relay Chat (IRC) servers have chat rooms in which people come together and chat with each other.

 Criminals use it for meeting co-conspirators

 Hackers use it for discussing their exploits/sharing the techniques

 Pedophiles use chat rooms to allure small children

**Cyber Stalking:**

In order to harass a woman her telephone number is given to others as if she wants to be friends with males

**Phishing:**

It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.

**Hacking:**

Hacking is a simple term which means illegal intrusion into a computer system without the permission of owner/user

**Denial of Services:**

This is an act by the criminal, who floods the bandwidth of the victim’s network or fill his e-mail box with spam mail depriving him of the services he is entitled to access or provide, or when internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

**E-mail Spoofing:**

A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

**Spamming:**

Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

**Cyber Defamation:**

This occurs when defamation takes place with the help of computers and or the internet. e.g. If someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

**Harassment & Cyber Stalking:**

Cyber Stalking means following every moves of an individual over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups etc.

**Salami Attack:**

When negligible amounts are removed and accumulated into something larger. These attacks are used for the commission of financial crimes. Criminal makes such program that deducts small amount like Tk. 3.50 per month from the account of all the customers of the bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but the criminal gains a huge amount.

**Intellectual Property Crimes:**

These include software piracy: illegal copying of programs, distribution of copies of software, copyright infringement: trademarks violations: theft of computer source code.

**Virus Attack:**

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves.

**E-mail Bombing:**

E-mail bombing means sending large number of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

**Logic Bomb:**

It is an event dependent program, as soon as the designated event occurs, it crashes the computer, releases a virus or any other harmful possibilities.

**Trojan horse:**

It is an unauthorized program which functions from inside and seems to be an authorized program, thereby concealing what it is actually doing.

**Data Diddling:**

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

**Forgery:**

The business world relies heavily on the production and exchange of legitimate documents to express legal rights and obligations, prove important facts, and exchange vital information. When these documents are falsified in any way, a crime known as forgery, social order and stability are challenged.

**Cyber Terrorism:**

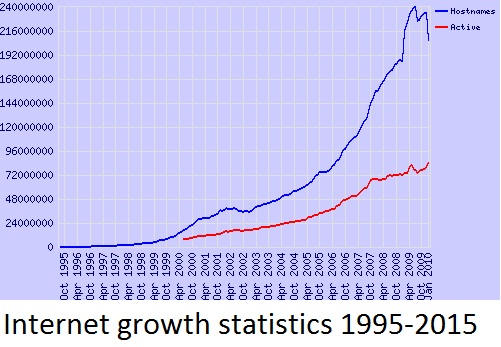
Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and where the information stored.

**Web Jacking:**

Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

**Brief History of using Internet in Bangladesh**

In late 1995, the government of Bangladesh invited applications to subscribe the VSAT (Very Small Aperture Terminal) data circuits and on June 4, 1996 the VSAT connection was commissioned and the internet was launched in Bangladesh for the first time and the first usage of internet was the publication of the National Polls Result in 1996. But this introduction could not create a good market at the very initial stage. After the year 1996, there were only two ISPs (Internet Service Providers) and about one thousand of users in the country. But the year 1997 is a landmark in this field as it recorded a tremendous advancement in internet using. The number of ISPs increased into twelve and users into ten thousand. Afterwards some new ISPs started their service which fuels the proportional advancement of his

sector. However, the government adopted more liberal national policies for a sustainable and rapid growth of this industry and as a result we had 180 ISPs by 2005. In 2006 Bangladesh got connected with Submarine Cable (SEA-ME-WE 4 Submarine Cable) which afforded big bandwidth and low cost than ever before. After this, over the years Bangladesh Telecommunications Company Ltd., BTCL (Now BTRC, ‘Bangladesh Telecommunication Regulatory Commission’) reduced the bandwidth price at regular intervals which attracted more and more users towards the internet world. As of now BTRC has about three hundreds and forty five (ISP Natiowide-94, ISP Central Zone-79, ISP Zonal-53, ISP Category A-99, ISP Category B-16, ISP Category C-04) registered ISP license Holders and there are approximately 4.5 million users connected to them which is about 0.32% of our total population.

**Present Scenario of Cyber Crime in Bangladesh**

Bangladesh does not have enough natural resources and has been trying to achieve the economic development through the utilization of ICT industry. Over the last few years, many nations have taken advantage of the opportunities afforded by ICT within a policy framework, laid down guidelines and preceded with the formulation of a national ICT strategy as a part of the overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development. The present government has also declared the vision-2021 i.e. within 2021 this country will become Digital Country and the per capita income will be equal to a middle income country. But the government as well as other concerns should consider crimes that may be committed in this world with the expansion of internet and other networks to convert this country into a digital country.

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been in India, Japan and China around since 3500 B.C. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime in the world history. A recent survey showed that a new cyber crime is being registered every 10 seconds in Britain. The situation of other countries in the world is almost the same and in some cases it is more critical and miserable. On July 4, 2009 two dozens of websites of South Korea and United States of America’s were under cyber attack and the attack was remarkably successful in limiting public access to victim web sites such as government web sites, treasury department, federal trade commission and secret service. They were continuously reporting problems days after the attack started during the July 4 holiday.

IT experts believe that about 90 percent of cyber crimes stay unreported. In case of Bangladesh, the situation is getting worsening day by day. The most common cyber attacks and crimes are listed below in Bangladesh:

1. Blackmailing girl by capturing their nude photographs and video on the sly and threatening to expose publicly. Such incidents are caused frequently by their boyfriends and others.

2. A number of community websites have been introduced, which the young girls and boys are using to exchange phone numbers for Posting hidden videos or even pictures with nudity etc.

3. Hacking in the website of Bangladesh Computer Society, which took place after a few days of a 3 day-long ‘Regional Seminar on Cyber Crime’ in Dhaka.

4. E-mail threatening the current Prime Minister Sheikh Hasina from a cyber cafe.

5. Hacking into the Internet account of Barisal DC office in 2003 AD, the incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Tar and Telephone Board (BTTB).

6. Hacking took place in the website of Bangladesh Rapid Action Battalion (RAB) in 2008, during the access to www.rab.gov.bd, the website read: "Hacked by Shahee\_Mirza."

7. Hacking the mail of BRAC Bangladesh13

8. Stealing the transaction report of Dhaka Stock Exchange through hacking.

9. Inserting naked pictures to the website of Bangladesh National Parliament.

10. Inserting naked pictures to the website of Jamate Islami Bangladesh.

11. Inserting naked pictures to the website of The Daily Jugantor.

12. E-mail threatening to World Bank Dhaka Office.

**Objectives**

The broad and general objective of this research is to find out and describe the nature of cybercrime by which the young people, who use Internet, are affected and the impact of it. This broad objective has been splinted into several specific objectives. These are,

1) To know the types of cybercrime by which the young people are affected;

2) To know the realization of victim about cyber crime; and

3) To know the effects of cybercrime upon the victims.

**Methodology**

The research has been conducted on Sylhet City Corporation in Bangladesh. Explorative research design has been used in this research to explore the real situation of cybercrime in this area and the consciousness of internet users (young) about this crime. The population of this research is not finite because internet users in cybercafés could not be counted. So, people who use internet (of age group 18 to 30) have been counted at several cybercafes in research area. Non-probability accidental sampling technique has been applied to select the sample because of the nonfinite population and the sample size is 30. Data have been collected through methodological triangulation method- Social survey (face to face interview with questionnaire) and case study to get in-depth information about the problem. After getting data, simple statistical tools like univariate analysis; mean, median and mode have been used to analyze data.

**3.1 Crime and Cyber Crime**

The crime committed in Cyber world is a common matter of present world. Basically Cybercrime is a complex crime and its range is so vast. There is no specific or all accepted definition of cybercrime because different agencies and researchers gave the definition according to their place and situation. It can say the cybercrimes are that crimes which have the involvement of computer and network (Fafinski 2008:2, Kowalski 2002:7, www. Definitions and general information [Cybercrime].htm).To given the definition of cybercrime some researchers told that the crime committed with internet and information technology (Sheridan 2004, Cybercrime - Wikipedia, the free encyclopedia.htm). It has some different name such as computer crime”, “computer-related crime”, “high-tech crime”, “Internet crime”( Brenner and Goodman 2002:6, Kowalski 2002:7). There are many types of cybercrime existing in present world. It is very difficult to find out all types of cybercrime because everyday the new dimension of cybercrime is inventing. We can cite few types of cybercrime, which occur generally in every place of the world. “Identity fraud” is a type (Blindell 2006:6, Fafinski 2008:4, ACPR 2006, parliamentary joint committee on the Australian crime commission 2004:43, Brenner and Goodman 2002: 7). It is defined as “The assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of actions” (Fafinski 2008: 4). Identity fraud is used as a means to commit drug, firearms and e-crime offences (parliamentary joint committee on the Australian crime commission 2004:44). Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity (ACPR 2006:14). In the United States of America, the term 'Identity theft' is generally used to cover all types of identity crime, The United Kingdom government appears to use 'identity fraud' as a generic term, In Australia, definitions adopted within policing entail the use of 'identity crime' as a generic description to cover all types of identity crime (ACPR 2006: 5). Another type of cybercrime is “Financial Fraud” (Fafinski 2008: 3, Graycer 2000: 8). It is defined as the use of deception for direct or indirect Financial or material gain (Fafinski 2008: 4). It includes Internet banking, credit and debit card fraud, and money laundering (Graycer 2000:8, parliamentary joint committee on the Australian crime commission 2004:47). In the context of credit card, financial fraud defied as “unlawfully obtained credit card numbers to order goods or services online” (Kowalski 2002:15). “Offences against the person” is a common type of cybercrime (Fafinski 2008: 3). It includes the use of a computer to cause an individual some form of personal harm such as anxiety, distress or psychological harm, precisely we can say threatening e-mails and the posting of derogatory information online is the best example of that crime (Fafinski 2008: 5). Another type “Computer misuse” means unauthorized access to a computer system such as “basic hacking”, “aggravated hacking” and unauthorized modification of computer material such as “viruses”(Fafinski 2008: 3). “Sexual offences” is most concerning types of cybercrime at present because of the availability of pornography (Fafinski 2008: 3). We can also give a relevant name that is “Pornography And Other Offenses Against Morality” it includes child pornography and other offenses against minors, stalking, harassment, hate speech etc (Brenner and Goodman 2002:10). This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual elements including pedophilic activity such as grooming a child for sexual activity. At present “Spam”, “Phishing”, “Bitnet’s” are the matter of concern at Cyber world because it causes lots of harm of computer system and data management (Jaishankar, Pang and Hyde 2007: 258). “Theft of Telecommunications Services” The "phone partakers" do it by gaining access to an organization’s telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Graycer 2000:1).

Telecommunications Piracy means the temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many (Graycer 2000:3).

**3.2 Effects of Cybercrime**

People in the whole world are affecting by cybercrime all time but most of the cases are unreported. In the UK there were 92,000 cases of online identity fraud during 2006. Around 40% of all identity frauds are facilitated online. The most stolen documents used by fraudsters were utility bills, passports and bank statements (Fafinski 2008: 8). 10% people in Australia suffered by on-line frauds (AFP 2006: 9). In 2000, of the 45,950 computer crimes reported by the NIBRS2, 5,744 were crimes where the computer was the tool and 40,211 were crimes where the computer was the object. The most common type of computer crime for both definitions was larceny/theft (Kowalski 2002: 12). Internet Crime Complaint Center (IC3) reported that 206,884 complaints were filed online for an estimated $239 million loss in 2007(www.crime-research.org/news/29.01.2009/3702) In Britain it is estimated that there were 207,000 cases of online financial fraud during 2006, among them Card-not-present (CNP) fraud was 49% and the total value of loss of CNP fraud are from £183.2M to £212.6M (Fafinski 2008: 10). About 42% financial frauds (Fraud, Credit Card, and Money Laundering) occurred in Australia during the year 2005 and 2006 (AFP 2007:7-9). In the Middle East over the past few years banks lost approximately one billion dollars to organized cybercrime on online transactions and most banks in the region are vulnerable to phishing attacks (El-Guindy 2008:16). UK banking association APACs warned that online banking fraud losses were £21.4m in the six months to June 2008(www.theregister.co.uk/2009/02/10/safer\_internet\_day/). FBI survey reported that the annual loss due to computer crime was estimated at $67 billion for U.S.A in 2005 (www.crime-research.org/news/29.01.2009/3702).

By the innovation of the Internet and the World Wide Web (WWW) has created a fictitious world filled with an unlimited amount of information, which dramatically changed the underground world of child pornography. By unexpectedly becoming the new medium for intent, motive, and ambition, the Internet has become a vital part of the child pornographer’s criminal tradecraft (Seigfried, Lovely and Rogers 2008:286-287). Half (49%) of Canadians have come across websites that contain pornography. Of those that have come across pornographic websites, 83% came across it unexpectedly and 46% found it offensive. 13% of Internet users came across content that promotes hate or violence to a particular group. 8% of Canadians who used the Internet had received threatening or harassing e-mail (Kowalski 2002: 15). Australian Federal Police reported that about 35% Child Pornography, 8% Child Grooming (using the internet and mobile phones), 4% Family Violence/Sexual Assaults occurred in Australia during the year 2005 and 2006 (AFP 2007:7-9). In Britain during 2008 there were 500 new cases of online child abuse reported every month (www.theregister.co.uk/2009/02/ 10/safer internet \_day). In Tahlequah a criminal took some pictures of undressed girls illegally and posted the pictures to their family and showed them exposing themselves, after proving that this criminal was accused and sent her to jail and financial punishment (www.crime-research.org/news/14.01.2009/3696/). In Britain 1,944,000 cases of online harassment placed during 2006 (Fafinski 2008: 12).

Cisco Systems Inc. found an alarming increase in the amount of personalized spam, which online identity thieves create using stolen lists of e-mail addresses or other poached data about their victims. Spam is growing quickly nearly 200 billion spam messages are now sent each day, double the volume in 2007 and that targeted attacks are also rising sharply. About 800 million messages a day are attempts are spear phishing in SANFRANSISCO (www.crime-research.org/news/18.12.2008/6381/). One in four (23 per cent) of UK internet users surveyed reckon either they or their close friends and family had been a victim of phishing scams during the last 12 months (www.theregister.co.uk/2009/02/10/safer\_internet\_day/). In Bangladesh, Prime Minister Sheikh Hasina got a threat by e-mail from a cybercafe and World Bank, Dhaka office got a threat through e-mail (Borhanuddin 2006:14).

Virus is the new dimension of cybercrime. About 6,000,000 virus incidents took place in Britain during 2006(Fafinski 2008:13). A virus named “Love Bug” which destroyed files and stole passwords. The virus was ultimately estimated to have affected at least forty-five million users in more than twenty countries. NASA and CIA also affected through this virus (Brenner and Goodman 2002:2).”Hacking” is a specific concept of stolen data and information from any computer through network. In Bangladesh lots of incident occurred during last year such as stolen the transactions report of Dhaka Stock Exchange, Hacking the e-mail of BRAC Bangladesh, Inserted porno movies in the website of Bangladesh national parliament, Jamate Islami Bangladesh, the Daily Jugantor (Borhanuddin 2006:14).

Theft of telecommunication services occur everyday in the world .Computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620,000 worth of international calls and Scotland yards had to responsible to pay that bill(Grayacer 2000:1). A hacker broke the voice-mail system of HUB Computer Solutions in Winnipeg and made calls worth of $43,000 and the company had to pay that unwanted bill (www.crime-research.org/news/24.12.2008/3684).Thieves hacked the Internet phone systems of WA businesses and used the phone system to make more than 11,000 international telephone calls in 46 hours that worth $120,000 and the Company paid that amount (www.crime-research.org/news/20.01.2009/3694/)

**Cyber Crime Characterized**

When internet was developed, the founding fathers of internet hardly had any idea that internet could also be misused for criminal activities. But the fact is that it is happening roughly and largely all over the world. Now the question is how these offences can be treated-whether through conventional or something extraordinary methods. If we have a deep introspection it will be proved that apparently there is no great difference between conventional crime and cyber crime.

The first demarcated difference line is the medium of committing the offence. Conventional crimes are prima facie territorial and occurred in physical world, but cyber crime is territorially unlimited and occurred in the world which is an electronic or virtual one. Some other major questions are raised regarding the nature of the cyber crime that whether it is a criminal offence or a civil wrong or tort. The answer would depend on the nature of the occurrence. After the ICT (Information and Communication Technology) Act, 2006 being passed all the aforesaid computer crimes are now treated as criminal offence.

**Scenario:**

American election properties have been stolen by the cyber intruders worth 400 million dollars. In June 2007 intruders hacked pentagon network. Recently in Bangladesh, 4 students of a private technology institute hacked the RAB web site. On 23 June 2009 RAB arrested JMB IT chief Rajib who used the internet as an engine of resources to make explosives to use in terrorism activities as he confessed that "I download information on explosives from internet, translate those in Bengali and send those to Mizan through Bashar (The Daily Star)," which is a serious concern for our national security.

In 2008 a petty hacker of Bangladesh named Shahi Mirza hacked the RAB’s website. Moreover he confessed to police that not only RAB’s website but also other national govt, and international site had been hacked by him for a long time. Totally he hacked 21 website together with Army’s website. So it is clear to us that the cyberspace of Bangladesh is not secured.

Few months ago Bangladesh government imposed restriction on opening you- tube video site because it contains an audio recording of a March 1 encounter between angry army officers and the prime minister. The recording was made on March 1 during an emotional meeting at the Dhaka cantonment. Hundreds of officers were present, distraught after paramilitary soldiers brutally killed more than 50 members of the army, including many of the leaders of the Bangladesh Rifles border force. Bangladesh government says in front of media that you-tube has been blocked in the interest of national security. In September 2007, most internet service providers (ISPs) in Bangladesh were affected by the Denial of Service (DoS) attack. A large volume of data packets was transmitted from an American data centre and caused server failure, slowing the performance of almost all ISPs. The attack was initially attempted on one ISP, Global Access Limited (GAL). Such attack causes serious damage. But our government remains silent after the attack and said in front of media that we have nothing to do.

**Cyber law in Bangladesh**

In the Information Communication Technology Act of Bangladesh does not define what the Cyber law by any section is. But Cyber laws are contained in the Information and Communication Technology Act, 2006. Therefore this Act provide the legal infrastructure for e-commerce others legal solution relating with cyber crime in Bangladesh. The said Act enables (a) Legal recognition of electronic transaction, (b) Legal recognition of digital signature, (c) Acceptance to con-tract expressed by electronic means, (d) e-commerce and electronic form, (f) publication of official gazette in the electronic form, (g) prevention of computer crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in e-commerce and electronic transaction, (h) and others solutions of the crime relation with information Communication Technology.

**Cyber Act 2006:**

To define and amend certain parts of law relating to legal recognition and security of information and communication technology and related matters the Information and Communication Technology Act- 2006 was enacted. According to the ICT Act the cybercrime shall be treated as non cognizable offence that is why the police cannot arrest the criminal without warrant except some Cases.

Chapter eight section 54 to 67 of the ICT Act 2006 describe the cybercrimes both civil and criminal matters. The followings shall be treated as crime;

- Unauthorized copying, extracting and downloading of any data, database

- Introduction of virus

- Damage and disruption to computer system and computer network

- Denial of access to authorized person to computer

- Providing assistance to make possible to commit to crime

- Hacking with computer system - Tampering computer source documents

- Electronic forger for the purpose of cheating and harming reputation

- Using a forged Electronic record

- Publication of digital signature certificate for the fraudulent purpose

- Confiscation of computer, network etc

- Publication of information which is obscene in electronic form

- Misrepresentation and suppressing material facts for obtaining digital signature certificate

- Breach of confidentiality and privacy

- Publishing false digital signature certificate

**Penalty or punishment:**

 If any person does any crime under section 54 of the ICT Act 2006 he will be given penalty of maximum 10 years rigorous imprisonment or fined up to 10 lacs taka or for the both of above.

 If any person does any crime under section 55 he will be given penalty of maximum 3years imprisonment or fined up to 3 lacs taka or with both. Whoever commits hacking under this act shall be punished of maximum 3 years imprisonment or fined up to 1 crore taka or with both.

 Whoever commits such crime under section 57 (uploading vulgar and obscene contents on website) of this act shall be punished of maximum 10 years imprisonment or fined up to 1 crore taka or with both.

 Penalty for failure to surrender license is 6 month imprisonment or fined up to 10 thousand taka or with both.

 Penalty for failure to comply with order made by the controller is maximum 1 Years imprisonment or fined up to 1 lacs taka or with both.

 Penalty for violation of the order of the controller in emergency period is maximum 5 years or fined up to 5 lacs or with both.

 Punishment for unauthorized access to protected system is the maximum 10 years or fined up to 10 lacs or with both.

 Penalty for false representation and hiding information is maximum 2 years imprisonment or fined up to 2 lacs or with both.

 Penalty for discloser of confidentiality and privacy is maximum 2 years imprisonment or fined up to 2 lacs or with both.

 Punishment for publishing false digital signature certificate is maximum 2 years imprisonment or fined up to 2 lacs or with both.

 Penalty for Publication of digital signature certificate for the fraudulent purpose is maximum 2 years imprisonment or fined up to 2 lacs or with both.

**Objectives of the ICT Act, 2006**

The objectives of the ICT Act, 2006 has been provided following purposes such as To smooth the progress of electronic filing of documents with government agencies and statutory corporations and to promote efficient delivery of government services by means of reliable electronic records.

To help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records. To facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce and so many others objectives have been included here.

Some identified Cyber Crimes as follows:



(i) Hacking or unauthorized entry into information systems  
(ii) Virus introduction  
(iii) Publishing or distribution of obscene content in electronic form  
(iv) Tampering with electronic documents required to be kept under the law  
(v) Frauds using electronic documents  
(vi) Violation of privacy rights such as STALKING  
(vii) Violation of Copyright, Trademark or Patent design  
(viii)Defamation through e-mail  
(ix) Holdings out threats through e-mail

Not only above mentioned cyber crimes are conducted but others are cyber crimes present before us. In future different types of cyber crimes will be intimated us.

**Weakness of the ICT Act, 2006**

The ICT law has some specific weakness. The law does sometimes regulate the social norm and then control of information technology. We can discus about the few weakness of the Act. Subsequently the law does give proper solution about the Intellectual Property Right and this law does not discuss of the rights and liability of domain name holders which is the first step of entering into the e-commerce. Not only these weaknesses of the Act but also others problems can to be brought through the Act.

**Advantages of Cyber law**

This Act has some disadvantages and also some advantages. This Act has provided us few advantages like as under the ICT Act, 2006, conduct important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the government at a later date. On the other hand Companies now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Subsequently this Act provided other facilities to run cyber or Information and Technology business.

However as Internet have grown in our country, the need has been felt to enact the appropriate cyber laws, which are indispensable to legalize and regulate Internet in Bangladesh. The existing laws of Bangladesh even with the most generous and moderate interpretation, could not be interpreted in the light of the promising cyberspace. We hope concern authority should take some steps to develop our existing cyber law.

**Issues on Cyber Act 2006:**

The Information Technology Act 2006 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

1. The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose. Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

2. Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime͟ – Mr. Pavan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the ICT Act 2006 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime.

3. Cyber torts- The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the ICT Act 2006 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the ICT Act 2006 read with the Penal Code is capable of dealing with these felonies.

4. ͞Cyber crime in the Act is neither comprehensive nor exhaustive͟- Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- ͞The IT Act, 2006 is Not comprehensive enough and doesn’t even define the term ͚cyber crime. Mr. Duggal has further commented, India as a Nation, has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes.’

5. Ambiguity in the definitions- The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The infamous "go2nextjob" has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the natives are till s. 66 exists in its present form. Further section 67 is also vague to certain extent. It is difficult to define the term \*lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by "the Bal Bharati case".

6. Uniform law- Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

7. Lack of awareness- One important reason that the Act of 2006 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling \*Microsoft pirated software\*over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for "online cheating" by buying Sony products using a stolen credit card.

8. Jurisdiction issues- Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2006 is very silent on these issues.

9. Extra territorial application- Though S.4 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

10. Raising a cyber army- by using the word ‘cyber army’ by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the "Cyber Crime Investigation Cell (CCIC of the Central Bureau of Investigation (CBI 11 “is definitely a welcome step in this direction. There are man cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –

 Case 1: When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

Status: Probe on

 Case 2: CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.

Status: Charge sheet not filed

 Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

Status: Pak not cooperating.

11. Cyber savvy bench- Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judge’s in today’s ǁord may be gathered by the statement- judges carve is to ͚law ought to be. Mr T.K.Vishwanathan, member secretary, Law Commission, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated ͞if there is one area of governance where IT can make a huge difference to India public is in the Judicial System”.

12. Dynamic form of cyber crime- Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, ͞In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind. “The (de-creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

13. Hesitation to report offences- As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the "Delhi time theft Case". ͞The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business.”This attitude of the administration is also reveled by incident that took place at "Merrut and Belgam". (For the facts of these incidents refer to naavi.com. For complete realization of the provisions of this Act a cooperative police force is require.

14. Time limitation- Chapter eight of the ICT Act creates a cyber tribunal to adjudicate of cybercrimes. The judge of the tribunal will complete the judgment procedure within 6 month of filing the case. The judgment will be given within 10 days from the date of finishing examination of witness or evidence or hearing.

**Some New Dimensions as Remedy against Cyber Crime**

No doubt technological defense is better than legal remedy in preventing hi-tech crimes, but there is always a chance of destruction of such defenses as these are not of perpetual nature. People who are more advance in technology than us can smash the security wall anytime. So, legal and other related remedies are obligatory to fight the war against the said circumstances. In addition to the present remedies the state can commence some new course of actions which are being trailed by some developed hi-tech state of the world. Let us have a glance at their features:

**I) Constitutional Safeguard:**

Bangladesh is a country of constitutional supremacy. Constitution plays the mother role in preserving and ensuring the rights and duties of both the state as well as the mass people. Constitutional provisions against cyber crimes may escort the cyber warfare to a national temperament which may result in a better form than any other organizational and legal remedy. Constitutional amendment may be the introducing procedure of such provisions.

**II) Special Wing of Police:**

For a digital Bangladesh, we need to equip our law enforcement agencies with training and technology to ensure peaceful cyber cloud. Cyber criminals are not the rivals of any specific country or of a region; rather they are the common enemies of the world. Citizens of the 21st century need to fight together against their common enemies. The rise of cyber crime insists the law enforcers to work as global police rather than regional or national police only. The Police Force through global partnership need to be able to meet the challenges of the technology to curb all crimes including Cyber Crime. U.K., U.S.A, India, Malaysia and some other developed countries have established special wings of police to combat the cyber war. Bangladesh can initiate such special police wings as a new armament against hi-tech threats along with other deterrent actions.

**III) Cyber Crime Agency by Government:**

On the last 23rd July of 2009 North Korea twisted ‘Korea Internet and Security agency’ 25, a government agency uniting three of its preceding internet technology organizations. Now, this agency will endeavor to make North Korea a stronger and a safe advanced country in using internet. India and some other countries have also created such agencies. Considering the present situation of using internet and increasing cyber crime in Bangladesh, Government can also commence such types of agencies. The worth of such agencies is that these will be able to perform multidimensional actions like advancing the internet infrastructure, maintaining the ISPs, fixing the internet using charges, preventing the cyber threats etc.

**IV) Watch Dog Group:**

These groups are enormously internet like the security oriented intelligence. They include capturing and receiving malicious software, disassembling, sandboxing, and analyzing viruses and Trojans, monitoring and reporting on malicious attackers, disseminating cyber threat information etc. This doggy concept is not a new one. ‘Shadow Server Foundation’ can be an example of Watch Dog Groups which was established in 2004. These may be individual as well as governmental. At present there is no such organization in Bangladesh, but in consideration with the escalating cyber threats, these doggy groups can be one of the vital constituents for developing Bangladesh as an advanced country especially in internet technology.

**V) Public Awareness:**

This course is no less important than technological precautionary actions, because most of the time common people become the victims of cyber threats and millions of computers are crashed away. So if it is possible to aware the populace about the nature, possible impairment and the antidote of the threats, it would be more convenient to defeat cyber criminals as well as save the virtual world and government can play the crucial role here. Like other vital issues, the government should create awareness among the mass people all over the country through different media. Besides, NGOs and other organizations can commence campaign in this regard.

**Legal response to cyber crime in Bangladesh**  
In order to facilitate e-commerce and encourage the growth of information technology, the ICT ct, 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or with both. However, recently our Parliament amended the ICT Act 2006, raising penalties for cyber crimes setting a minimum of 7 years imprisonment and a maximum of 14 years or a fine of Tk. 1 crore or both. The bill made offences under sections 54, 56, 57 and 61 of the ICT Act, 2006 cognizable and non-bail able, empowering law enforcers to arrest anyone accused of violating the law without a warrant, by invoking section 54 of the Code of Criminal Procedure. All such offences were non-cognizable in the ICT Act, 2006. However, all concerned apprehend of the misuse of the power by the police.  The ICT Act, 2006 as amended in 2013 is obviously a brilliant achievement of Bangladesh in the field of cyber law. Critics point out that still there remain certain specific limitations of the said Act as under.   
(1)    The Act remains silent about various intellectual property rights like copy right, trade mark and patent right of e-information and data.  
(2)    The enactment has a major effect on e-commerce and m-commerce in Bangladesh. But it keeps itself mum as to electronic payment of any transaction.  
(3)    The legislation was initially supposed to be applied to crimes committed all over the world; but nobody knows how this can be achieved in practice.  
(4)    Spamming has become a peril in the west as such they have made anti spamming provisions in cyber law. However, there is no anti spamming provision in our Act.  
(5)    Domain name is the major issue which relates to the internet world thoroughly. But the ICT Act, 2006 does not define ‘domain name’ and the rights and liabilities relating to this.  
(6)    The Act does not address any crime committed through using mobile phones.  
(7)    This law made e-mails as evidence, conflicting with the country’s Evidence Act that does not recognize as e-mails as evidence.  
We hope our government would take proper initiative to get rid of the problems for ensuring a cyber crime free peaceful society.

**AIMS AND OBJECTIVE:**

As cybercrime incidents are on the increase, and it menace is affecting both Government organizations, Individuals and businesses, the main aim of this research will be to find out the truth which about cybercrime that is hidden and which has not been discovered as yet as it relate to the rate of increase, the sophistication of attack, motivation of the cybercriminals and ultimately find a way of reducing cybercrime activities and it effect on businesses to the barest minimum. Where prevention and control is not totally possible, the research will focus on deterrent measures like recommending maximum and appropriate punishment for offenders. In this regard, the research will review the existing law and suggest amendments where necessary, develop a detail and acceptable measures of tracking the cyber criminals (tracing the hacker to the cyber space). Cyber Forensic techniques are the deal here. The research will be both descriptive and exploratory or formulate in nature.

## Cybercrime Markets

The Internet allows for illicit markets to be created and maintained. The Internet provides its users with an opportunity to hide their identities and to be in remote locations to create and be part of illicit markets. For instance, cybercriminals can use different Web sites to trade (i.e., buy or sell) merchandise illegally through legitimate sources (e.g., eBay) or through illegal sites. Some of these Web sites are not able to be traced back to their original sources. While a host of illicit markets exists (e.g., illegal adoptions, surrogate mothers, egg donors, obtaining banned substances, organ donors thieves, forbidden animals, endangered species, and illegal gambling), four markets will be discussed here.

One of the most pervasive forms of cybercrime is digital piracy (Gopal, Sanders, Bhattacharjee, Agrawal, & Wagner, 2004). Digital piracy is defined as the illegal act of copying digital goods, software, digital documents, digital audio (including music and voice), and digital video for any reason without explicit permission from and compensation to the copyright holder (Gopal et al., 2004; Higgins, Fell, &Wilson, 2006). The Internet has facilitated an increase in digital piracy in recent years. Wall (2005) notes four characteristics of the Internet that have enabled individuals to easily commit criminal activity: It allows anonymous communication, it is transnational, it has created a shift in thinking from the ownership of physical property to the ownership of [ideas](http://research-paper.essayempire.com/topics/), and it is relatively easy. In addition, Wall contends that the Internet facilitates piracy because it allows the offense to take place detached from the copyright holder, which provides the offender with the perception that the act is victimless.

Several researchers have acknowledged sub forms of digital piracy (i.e., audio and video piracy) as being increasingly pervasive (Gopal et al., 2004; Hinduja, 2003). Higgins et al. (2006) defined audio and video piracy as the “illegal act of uploading or downloading digital sound or video without explicit permission from and compensation to the copyright holder” (p. 4). Technological advancements are partly responsible for the increased ease and accessibility of digital piracy. The International Federation of Phonographic Industries (IFPI) (2006) estimates that one in three music discs purchased around the world are an illegal copy. The IFPI further estimates that 37% of all CDs purchased in 2005 were pirated, resulting in 1.2 billion illegal copies purchased worldwide. In fact, the IFPI [concludes](http://research-paper.essayempire.com/writing/how-to-write-a-conclusion-for-a-research-paper/) that pirate CD sales outnumbered legitimate CD sales in 30 markets across the world and resulted in a loss of $4.5 billion from the music industry.

Similar issues take place in the context of the movie industry. To be clear, industry figures indicate that the costs of unauthorized copying and redistribution of movies via physical media (e.g., video cassettes, DVDs, VCDs, etc.) exceed several billion dollars annually. In 2005, the Motion Picture Association of American (MPAA) reported that over 90% of the movies that are initially pirated are due to the use of cam cording in movie theaters. The Internet has allowed movie pirates to be able to illegally download movies (MPAA, 2004). In 2004, the MPAA reported that $2.3 billion were lost due to Internet piracy.

Several researchers have argued that college students are likely to pirate almost all forms of digital media (Hinduja, 2003; Higgins et al., 2006). This includes software piracy. According to the Business Software Alliance (BSA, 2007), the trend of piracy among college students has been going up slightly compared to 2003 and 2005 rates. Importantly, two thirds of the students surveyed still believe that it is okay to swap or illegally download software without paying for it (BSA, 2007).

Since the Copyright Act of 1976, digital piracy has been a criminal act (Higgins et al., 2006). Mass copyright violations of movies and music were made a felony offense in 1982 by the Piracy and Counterfeiting Amendments Act, which was amended to include the distribution of copyrighted materials over the Internet via the No Electronic Theft Act (Koen & Im, 1997). That is, when an individual proceeds to burn an extra copy of a music CD, download music from the Internet without paying, or use a peer-to-peer network to download music information, he or she is pirating music. This is especially true for digital music piracy that is committed through a multitude of mode operandi (e.g., CD burning, peer-to-peer networks, LAN file sharing, digital stream ripping, and mobile piracy [see <http://www.IFPI.org> for a discussion of these techniques]). The penalties for these acts may be civil (e.g., $10,000 per pirated copy) as well as criminal (e.g., possible jail sentences) (Koen & Im, 1997).

Cybercrime includes the promotion and the distribution of pornography. When done over the Internet, this is known as cyber pornography. While viewing pornography may not be criminal for those who are of age, the Internet does not discriminate based on age. That is, teenagers’ fantasies about nudity may easily be replaced by hardcore pornographic images of every conceivable sexual activity.

In the academic literature, some researchers have shown that access to and viewing of cyber pornography is a behavior that is increasing. Ybarra and Mitchell (2005) used data from kids and young adults to examine exposure to cyber pornography. They showed that individuals that sought out cyber pornography were likely to be male, 14 years old and older, and more depressed, whereas those younger than 14 were more likely to be exposed to pornography through traditional means—movies and magazines.

Others have shown that cyber pornography is not just for teenagers, making the behavior non–age specific. Stack, Wasserman, and Kern (2004) used the General Social Science Survey to examine who viewed pornography using the Internet and the reasons why. They showed that individuals that had weak religious ties, unhappy marriages, and past sexual deviance are more likely to view pornography via the Internet. Buzzell (2005) examined the factors that influence access to cyber pornography. The study showed that when employment status increases, technology does play a role in the access to cyber pornography.

The Internet allows cybercriminals to participate in underage liaisons. One form of this particular type of cybercrime is the online solicitation of children for sex. This is exploitation that involves an adult who engages in discussion with a child online and uses his or her manipulation skills to coerce the child to meet in person for sexual purposes. Importantly, the number of children that are approached on the Internet for these types of offenses is staggering. Finkelhor, Mitchell, and Walk (2000) showed that 1 out of every 5 youths is solicited by someone online for sexual relations.

The anonymity of the Internet allows cybercriminals to disguise their postings, responses, and identities. This affords the cybercriminals the opportunity to disappear at a moment’s notice. In short, the Internet allows cybercrimes to be performed more easily and simply while making criminals’ detection, apprehension, and prosecution more difficult. Therefore, the Internet makes cybercrimes through illicit markets more difficult to examine.

**Conclusion**

At present we are a developing country and trying our best to be a developed one. In order to digitalize Bangladesh there is no alternative to secured technological advancement among which tenable internet using should prevail in priority. This advancement demands ICT experts of which we have great lacking. The state should move forward for creating such experts with indispensable national ventures. Besides this statutory shields should be made most effective by executing the aforesaid course of actions. Finally, we have to remember that technology is such a thing which is changing its nature and direction every moment and we have to achieve the maximum capability to fight its change in every moment change both in physical and virtual world for a perpetual existence.

From the research we got the maximum Internet user are student (Table 4) and they use for their study purpose and many more. So we can say that in Sylhet the Internet user are limited in student community because, to use internet a person has to be knowledgeable about computer operation. We find few people gave their details to some tempting offers (Table 9). It is very interesting that who gave information to those sites thought that the offer is fake but they can not imagine that someone has stolen their identity. Among the respondent most people have no intention to get any thing by different tempting offer because they thought it’s not for them, may be they can’t afford that or something else. We got more than half (56.7%) (Table 8) Internet users owned land phone but they did not victimize through theft of telecommunication service. There is more than half (60%)(Table 12) users use on-line banking that’s mean on line banking is going to popular to young people because of its easy access but yet now no one lost any money through financial fraud. So we can say that because of rising on-line banking facility we should develop the consciousness about such type of cybercrime to save our nation’s money. We find that the practice of e-mail threat, neglecting message about religion, political parties etc doesn’t start here yet so no one has any experience about that. We know hacking is now most useable concept in cybercrime topic but in Sylhet district accept 1 respondent no one has that bad experience but we can’t say that no hacking occurred in this cyber area because most of time users can’t identify that he/she has been hacked by others. We see among the respondent more than three out of five (70%) (Table 15) people owned personal computer at their home and people use Internet who has no computer at home. It is clear that most of the people keep in touch with Internet so it is a good site of technological advancement. Most of the respondents reported that different types of virus affect their PC and they lost lots of valuable data and sometimes windows crash occurred. Most of the users use anti-virus software for virus protection but among them 68.8% computer owner don’t update anti-virus so their attempt of prevent virus is practically doesn’t work properly because everyday new viruses introduce in cyber world. So if they only use anti-virus without updating that will be fruitless and maximum users do that. We find 70% respondents gave their information to different social websites like www.facebook.com, www.hi5.com etc. Users said that they put the correct information on these websites but we know at present some hackers break down these websites protocols and can theft lots of information of different people and it is being doing now. So because of hacking of these sites general people may suffer for losing identity and it can occur without user’s activity.

Therefore, it can be said that the young Internet users in Sylhet city don’t affect by different cybercrime accept computer misuse but we can’t say that most users are so conscious about the cybercrime. We find that most of the people have little idea about cybercrime and because of that they can’t identify their position in Cyber world. In present world, third world countries are more choice able to cybercriminals because they can do cybercrime here easily. So, as staying at the first stage of the network world, government should perform some activities to make people conscious about cybercrime. If we reduce the affect of cybercrime in our country that will be a great achievement for us, and this success not for the peoples only it’s for the nation. Now it’s the time to come forward and enter into the digital world with full protection and safety.

The policy maker may formulate a baseline security procedures policy outlining the minimum requirements which must be met by agencies regarding information security and may also develop a special analysis site which will be observed 24/7 and will provide real-time monitoring of cyber activities.

“Cyber incident response unit “ an ‘a cyber crime investigation cell’ may be built within law enforcement authority to fight cyber crime successfully by adopting the enhancing capacity, good police work, skilled investigators sharing the ‘too few ‘professionals skilled in cyber-security and by training new officers to become experts in the field and providing adequate logistic support/equipment.

Moreover, to keep the national security uninterrupted and avoid hacking, web servers running public sites must be physically separate protected from internal corporate network and web site owners should watch traffic and check any inconsistency on the site by installing host-based intrusion detection devices on servers.

Finally, we can say that the collective effort of state and nations is only a possible way to see the peoples͛ dream of a Digital Bangladesh in existence and could protect individuals and national security of the state from the aggression of cyber criminals.

**References**

ACPR. (2006). Parliamentary joint committee on the Australian crime Commission. Retrieved from http://www.acpr.gov.au./pdf/ACPR145\_2.pdf

ACPR. (2006). Standardisation of definitions of identity crime terms: A step towards consistency. Retrieved from http://www.acpr.gov.au./pdf/ACPR145\_3.pdf

Baker, T. L. (1994). Doing Social Research (2nd ed.). Mc Graw-Hill, Inc, Singapore. Blindell, J. (2006). Review of the legal status and rights of victims of identity theft in Australasia. Retrieved from http://www.acpr.gov.au./pdf/ACPR145\_2.pdf

Borhanuddin, A. R. M. (2006). Cybercrime and Bangladesh perspective. Retrieved from http://www.scribd.com/doc/3399476/cyber-crime

Brenner, S. W., & Goodman, M. D. (2002). Cybercrime: The Need to Harmonize National Penal and Procedural Laws. Retrieved from http://www.isrcl.org/paper/brenner.pdf

Convention on Cyber-Crime. (2001). The Convention on Cyber- Crime, a unique instrument for international co-operation. Budapest: Council of Europe. Retrieved from http://conventions.coe.int/treaty/EN/projets/projets.htm

El-Guindy, M. N. (2008). Cybercrime in the Middle East. Retrieved from www.cybercrimejournal.co.nr

Etter, B. (2002). Cybercrime: now this changes everything! Retrieved from http://www.acpr.gov.au/pdf/presentations/netalertdec02.pdf

Fafinski, S. (2008). UK Cybercrime report Retrieved from http://www.garlik.com

Gjata, O. (2007). Cybercrime. Retrieved from http://mason.gmu.edu/~ogjata/index.html

Graycar, A. (2000). Nine types of cyber crime. Retrieved from http://aic.gov.au/conference/other/graycer\_adam/2000-02-cybercrime.html

Hammadi, S. (2008). A click away from crime. Retrieved from http://www.prp.org.bd/Media/14-20March08.pdf

Hossain, A. (2004). Access to Internet: Bangladesh Perspective. Retrieved from http://www.mosict.gov.bd

Kowalski, M. (2002). Cyber-Crime:Issues, Data Sources, and Feasibility of Collecting Police-Reported

Statistics. Catalogue No. 85-558-XIE, ISBN 0-660-33200-8. Retrieved from http://statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf

Morris, S. (2004). The future of netcrime now: Part 1 - threats and challenges. Retrieved from

http://www.homeoffice.gov.uk/rds/pdf04/rdsolr6204.pdf

Nachmias, & Nachmias. (2002). Research Methods in the Social Sciences. St Martin Press Inc. Fifth Avenue, New York, NY-10010.

Reynolds, P. D. (1976). A Primer In Theory Construction. The Bobbs-Merrill Company, Inc.

Seigfried, K. C., Lovely, R. W., & Rogers, M. K. (2008). Self-Reported Online Child Pornography Behavior: A Psychological Analysis. Retrieved from http://www.cybercrimejournal.co.nr

Young, K. (2008). International journal for cyber criminology. Retrieved from www.cybercrimejournal.co.nr/

**Appendix. Tables**

Table 1. Age of respondent

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| 18-22 | 10 | 33.3 |  |
| 23-26 | 12 | 40.0 | 23-26 |
| 27-30 | 8 | 26.7 |  |
| Total | 30 | 100.0 |  |

Table 2. Sex of respondents

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Male | 28 | 93.3 |  |
| Female | 2 | 6.7 | Male |
| Total | 30 | 100.0 |  |

Table 3. Educational status

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| SSC | 1 | 3.3 |  |
| HSC | 7 | 23.3 |  |
| Honours | 16 | 53.3 | Honours |
| Masters | 6 | 20.0 |  |
| Total | 30 | 100.0 |  |

Table 4. Occupation of respondent

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequen | Percent | Modal catego |
| Student | 19 | 63.3 |  |
| Service holder | 5 | 16.7 |  |
| Private service | 5 | 16.7 | Student |
| Unemployed | 1 | 3.3 |  |
| Total | 30 | 100.0 |  |

Table 5. Duration of use internet

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Freque | Percent | Modal catego |
| 1 -3 | 10 | 33.3 |  |
| 4 -6 | 12 | 40.0 | 4-6 |
| 7 -10 | 8 | 26.7 |  |
| Total | 30 | 100.0 |  |

Table 6. Regularity of use

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal catego |
| Yes | 22 | 73.3 |  |
| No | 8 | 26.7 | yes |
| Total | 30 | 100.0 |  |

Table 7. Reason of internet use

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Modal cate | Percent |
| Study | 4 | 13.3 |  |
| Job | 5 | 16.7 |  |
| Various pu | 20 | 66.7 |  |
| Private | 1 | 3.3 |  |
| Total | 30 | 100.0 |  |

Table 8. Owning land phone

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 17 | 56.7 |  |
| No | 13 | 43.3 | Yes |
| Total | 30 | 100.0 |  |

Table 9. Giving information at any offer in internet

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Freque | Percen | Modal cate |
| Yes | 7 | 23.3 |  |
| No | 23 | 76.7 | No |
| Total | 30 | 100.0 |  |

Table10. Types of given information at any tempting offer

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Name and address | 2 | 28.6 |  |
| 1 and bank account information | 1 | 14.3 |  |
| Additional information | 4 | 57.1 | Additional information |
| Total | 7 | 100.0 |  |

Table 11. Reason of not giving information

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Don’t believe | 14 | 46.7 |  |
| Don’t understand | 2 | 6.7 |  |
| No reason | 7 | 23.3 | Don’t believe |
| Total | 23 | 76.7 |  |

Table 12. Use online banking

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 18 | 60.0 |  |
| No | 12 | 40.0 | Yes |
| Total | 30 | 100.0 |  |

Table 13. Any neglecting message in internet

|  |  |  |  |
| --- | --- | --- | --- |
| Category | YES | NO | TOTAL |
| Getting erotic info about yourself | 0 | 30 | 30 |
| Getting threat through e-mail | 0 | 30 | 30 |
| Neglecting message about religion | 0 | 30 | 30 |
| Neglecting message about political ideology | 0 | 30 | 30 |

Table 14. Affected through hacking

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 1 | 3.3 |  |
| No | 29 | 96.7 | No |
| Total | 30 | 100.0 |  |

Table 15. Owning a computer

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 21 | 70.0 |  |
| No | 9 | 30.0 | Yes |
| Total | 30 | 100.0 |  |

Table 16. Affected through virus

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 20 | 95.2 |  |
| No | 1 | 4.8 |  |
| Total | 21 | 100.0 | Yes |

Table 17. Times of virus attack

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Few | 4 | 19.0 |  |
| Average | 2 | 9.5 |  |
| Many | 15 | 71.4 | Many |
| Total | 21 | 100.0 |  |

Table 18. Disclose information of respondent

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 1 | 3.3 |  |
| No | 29 | 96.7 | No |
| Total | 30 | 100.0 |  |

Table 19. Access Social Websites

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 21 | 70.0 |  |
| No | 9 | 30.0 | Yes |
| Total | 30 | 100.0 |  |

Table 20. Putting correct information

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 20 | 95.2 |  |
| No | 1 | 4.8 | Yes |
| Total | 21 | 100.0 |  |

Table 21. Mentality about the web offers

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Percent | Modal category |
| Yes | 6 | 20.0 |  |
| No | 24 | 80.0 | No |
| Total | 30 | 100.0 |  |