ISSN 2218-2578
Volume I (2010) *The Northern University Journal of Law*

Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies

Ashiquddin Mohammad Maruf[*]
Md. Rabiul Islam[**]
Bulbul Ahamed[***]

1. Introduction

With the advent of technology human beings are becoming exclusively dependant on automation and we can see its influence on all spheres of our life. The history of automation began when Babbage invented computer and especially a new horizon was opened before us with the invention of network particularly the Internet and World Wide Web (WWW). Internet has become the backbone of all kinds of communication systems and it is also one of the most important sources of knowledge in the present digitalized world.

It is a *network of networks* [1] that consists of millions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The World Wide Web is a huge set of interlinked documents, images and other resources, linked by hyperlinks and URLs.

The internet allows computer users to connect to other computers and to store information easily across the world. They may offer to do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This free access to network creates previllages to some highly skilled criminals to do illegal deeds in the cyber world. The most common evil doings are crashing a computer system, theft of information contained in electronic form; e-mail bombing, data diddling, financial fraud like unlawful transfer of money by breaking the security code of credit cards, denial of services and virus attack. But the prevention and remedy for these

[*] Senior Lecturer, Department of Law, Northern University Bangladesh (NUB), E-mail: ammaruflaw@gmail.com

[**] Senior Lecturer, Department of Business Administration, Northern University Bangladesh (NUB), E-mail: rabi_cpi@yahoo.com

[***] Senior Lecturer in CSE, Department of Computer Science and Engineering, Northern University Bangladesh (NUB), E-mail: bulbul2767@yahoo.com

[1] Peter Norton, *Introduction to Computers*, Fifth Edition, (Career Education) 2002, p. 23

offences through the structural and legal framework are inadequate in our country.

2. 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.[2] 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 this 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[3] and there are approximately 4.5 million users connected to them which is about 0.32% of our total population.

3. Cyber Crime Defined

It is a technological crime and a misnomer[4] term. It is also known as computer crime, electronic crime, hi-tech crime and e-crime. Actually it involves a

[2] Hamidur Rashid, *Internet History of Bangladesh*, http://ezinearticles.com/?Internet-History-of-Bangladesh&id=2327010, last visited 01.10.2009.

[3] Summary of- BTRC licenses, http://www.btrc.gov.bd/licensing/operators/summary_of_licenses.pdf , Last visited 06.09.2009

[4] A.R.M Borhanuddin, *Cyber Crime and Bangladesh Perspective*, Available Online: http://www.scribd.com/doc/3399476/cyber-crime**,** last visited 06.09.2009.

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:[5]

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**:**[6]

- 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 commited against the above mentioned groups:

Against Individuals:-

a) Hacking or Cracking
b) Illegal/Unauthorised access

[5] Computer Crime, Wikipedia**,** http://en.wikipedia.org/wiki/Computer_crime, last visited 15/08/2009.

[6] Classification of Cyber crime**,** Report Cyber crime, http://www.reportcybercrime.com/case_study_details_user.php**,** last visited 12/09/2009.

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) Indecedent 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) Intelluctual property crimes
c) Internet time theft

Against Organizations:-

a) Unauthorised 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) Vandalising the infrastructure of the network

Against Society:-

a) Forgery

b) Online gambling
c) Trafficking
d) Pornography (specially 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
- Paedophiles 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.

4. 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 proceeded 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.[7]

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

[7] Clause 1.3 of the National Information and Communication Technology (ICT) Policy (October, 2002), at http://sdnbd.org/sdi/issues/IT-computer/itpolicy-bd-2002.htm, Last visited 12/09/2009.

remarkably successful in limiting public access to victim web sites such as government web sites, treasury department, federal trade commission and secret service.[8] 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.[9]
4. E-mail threatening the current Prime Minister Sheikh Hasina from a cyber cafe.[10]
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).[11]
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."[12]
7. Hacking the mail of BRAC Bangladesh[13]
8. Stealing the transaction report of Dhaka Stock Exchange through hacking.[14]

[8] *Full-Scale July 4th Cyber Attacks Waged Against U.S., S. Korean Gov. Sites,* at http://chattahbox.com/technology/2009/07/08/full-scale-july-4th-cyber-attacks-waged-against-us-s-korean-gov-sites/, Last visited 17/11/2009.

[9] Bangladesh Computer Society Website Hacked By Libyan Hacker, Staff Reporter Shah Jalal Shimul, DNews, http://www.cnewsvoice.com/DNews.php?NewsID=N000000770, Last visited 11/11/2009

[10] The Daily Star Web Edition Vol 5 Num 94, http://www.thedailystar.net/2004/08/27/d4082701055.htm, Last visited 11/11/2009.

[11] The Daily Star, Sunday, July 13, 2003

[12] http://www.thedailystar.net/archive.php?date=2008-09-06, Last visited 10/10/2009.

[13] *Supra Note* 4

[14] *Ibid*

9. Inserting naked pictures to the website of Bangladesh National Parliament.[15]
10. Inserting naked pictures to the website of Jamate Islami Bangladesh.[16]
11. Inserting naked pictures to the website of The Daily Jugantor.[17]
12. E-mail threatening to World Bank Dhaka Office.[18]

5. Cyber Crime Characterised

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.[19] 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.

6. Remedies Available and their Lacking

A proverb goes ‘Prevention is better than cure’. For prevention of numerous cyber crimes it is better to initiate advanced technological actions. These are technological precautionary affairs for prior prevention. We will rather try to find out the legal and other remedies and their lacking available in Bangladesh for curing the alleged cyber crimes. A cyber victim in Bangladesh has a better opportunity to get the proper remedy under the ICT Act, 2006. This statute is the first and the only door open for the lawful remedy of numerous cyber crimes in Bangladesh. Through this statute it is being tried to locate all the

[15] *Ibid*
[16] *Ibid*
[17] *Ibid*
[18] *Ibid*
[19] *Ibid*

probable grounds of cyber crime frequently occurring at present and which might occur in future as well like damaging any computer or computer system, hacking, spreading viruses and false information, causing defamation through the internet, changing the source code, stealing or damaging any text, audio, video documents etc. Provisions for special Cyber Tribunals[20] (both Original and Appellate) and punishments of lighter/severe form have been fixed.

In addition to the above mentioned remedies it is also noted that even after three years of passing this Act not a single case is filed under this law. Mass people are not so aware about such types of new crimes and the procedure of their remedy. One of the causes of this may be that no Cyber Tribunal and Cyber Appellate Tribunal have been formed by the government yet. Moreover as per the provisions of the ICT Act a good number of other procedural and structural hurdles also exist which are as follows:

Firstly, a session judge or an additional session judge will preside over the Cyber Tribunal[21] and a bench of three members including a chairman who will be an ex or acting judge or a competent person to be a judge of Supreme Court and an ex or acting Dist. Judge and an ICT expert, two other members of the bench, will preside over the Cyber Appellate Tribunal[22] and like the other criminal cases Public Prosecutors will prosecute on behalf of the state in this regard. The problem is that judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the opportunity to be assisted by the ICT expert. But is it possible to give the verdict on the basis of another’s knowledge? The reality in our country is that so far no initiative is taken by the government to train up the judges for acquiring the minimum technological knowledge required for ensuring justice.

Secondly, a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer)[23] regarding the cyber crimes. Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal.

[20] The Information and Communication Technology Act-2006, Sec: 68, 82.

[21] *Ibid,* Sec:68(2)

[22] *Ibid* Sec:82(2)(3)

[23] *Ibid* Sec: 69(1)

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

Thirdly, the government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of those proposed tribunals.[24] Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state.

Proper execution of statutes ensures the rule of law. Circumstances say that inadequate execution of the ICT Act, 2006 is one of the root causes for the increasing cyber crimes in Bangladesh. The solution of those aforementioned problems demands that the state must take nippy steps along with logistic and financial assistance.

7. 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

[24] *Ibid,* Sec: 82(4)

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

[25] Korea Internet and Security Agency, at http://www.nida.or.kr/kisa/eng/english_ver.html, Last visited: 10/11/2009

media. Besides, NGOs and other organizations can commence campaign in this regard.

8. 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.