Exploration of Cybercrime and Cyber Law: Growth of the State Concerns and Initiatives with Special Focus to the Context of Bangladesh

Md. Abu Hanif[1]

***Abstract*:** Tomorrow's terrorists may be able to do more damages with a key board than with a bomb. This piece of writing seeks to talk to and analyze the concept of cybercrime and its emergence addressing at the national and international levels. It reviews the existing legislative and regulatory framework and their effectiveness in fighting this form of borderless and organized crime taking the South Asian country Bangladesh as a case study. *Finally*, the article concludes with some preventive and punitive measures in the battle against cybercrime

***Keywords*:** Cyber space, cyber crime, conventional crime, UNCITRAL, cyber ethics.

Introduction

We are breathing in the 21st century with a panic where cyber space exists having enormous benefits as well as danger of information technology. This Cyber reality incorporates and performs most of the official, non-official, financial, non-financial and many of our real life activities using computer and computer related devices viz. e-banking, e-commerce, e-learning, e-foreign trading, networking, e-industrial infrastructures, telecommunications, e-air traffic control, e-ticketing, e-*krishi*, e-global positioning systems, e-global distribution systems and hi-tech medical equipment etc which make our lives easier, dynamic, time and labor saving. Alongside many of these advantages, there are dangerous risks with using these technologies. These are committing cybercrimes in different forms such as: data diddling, electronic fraud in the financial sector, identity theft, illicit use of valuable information, hacking or cracking, cyber-stalking, distribution of pirated software, terrorism,

[1] Lecturer, Department of Law & Justice, Bangladesh University of Business and Technology (BUBT), Dhaka, Bangladesh. E-mail: abuhaniflaw@yahoo.com

interference with sophisticated high level national security measures, immoral activities, defamation and harassment, blasphemy, intellectual property rights infringements and so on which affect individuals at large. It is said the modern thief can steal more with a computer than with a gun (Hackerman & Robert, 1991). Many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe mentioned cybercrime as a major concern for the global community (Chawki, 2005). These crimes should not be continued rather stopped for the proper enjoyment of the blessings of modern digital world. Owing to a new phenomenon having peculiar features in the field of crime, investigation of its ins and outs, to make the relevant laws apply properly to the particular crime, demands badly.

Objectives of the Study

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

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

Contribution and Relevance of This Research to the Field of Cyber Law

Cybercrimes are becoming serious problems that are affecting the whole nation like many other countries of the world. But the existing penal or criminal laws are incapable to take action quickly against cyber crimes. However, certain efforts have been made by the Government to curb the cybercrimes by enacting several acts, means and policies though there remain certain shortcomings. This article aims to thrash out the scenario of cybercrime and the national, regional and global status of cyber laws and unveil those shortcomings and puts appropriate suggestions to meet the challenges of preventing the different kinds of cybercrimes which

will be very much helpful for legislature, law enforcers and the persons involving the usage and study of the on-line or related devices.

Methodology and Data Sources

Bearing in mind the nature, analytical and empirical research method has been resorted to complete this work. Primary and secondary sources of data have been taken into consideration for the purpose. The references have been adopted from national and international updated statutes, books of famous writers, articles published in credible journals, decided cases, research reports, acts, newspapers and websites etc. In course of this research, some renowned cyber jurists and computer engineers have been interrogated to know their views about cyber crimes and cyber related technical & legal issues.

Cyber Related Conceptual Issues; Their Varying Forms, Natures and Aspects

Cyberspace is the virtual environment in which communication over computer networks occurs. The term was first used in science fiction and cinema in the 1980s, was adopted by computer professionals and became a household term in the 1990s. During this period, the uses of the Internet, networking, and digital communication were all growing dramatically and the term 'cyberspace' is able to represent the many new ideas and phenomena that are emerging (Goodman & Brenner, 2002). Criminal activity committed on the Internet or cyber space is termed cyber crime. In Dictionary, 'Crime' refers to the activities that involve breaking the law (Hornby, 2010). 'Cyber crime' is a crime involving the use of computer, such as sabotaging or stealing electronically stored data (Garner, 2004). It be unlawful act where in the computer is either as a tool or target or both (Nagpal, 2009). This crime is committed mainly against individual or organization, Government in a network environment or on Internet i.e. cyber space.

The perception of cyber crime is not fundamentally different from the concept of conventional crime but peculiarity due to the different ways and means of committing cyber crime makes it to somehow challenging. Both include conduct whether act or omission which cause breach of rules of law and counter balanced by the sanction of the state. To evaluate the specialty of cyber crime it is obvious that the distinctive features of conventional crime and cyber crime be discussed- 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 committed in physical world, but cyber crime is territorially unlimited and committed in the world which is an electronic or virtual one. Unlike the traditional crime, cybercrime is a global crime as a European Report explains: 'computer-related crimes are committed across cyber space and do not stop at the conventional state-borders. They can be perpetrated from anywhere and against any computer user in the world (Goodman & Brenner, 2002).

Cyber laws that prevent and reduce large scale damage from cybercriminal activities by protecting information access (Janssen, 2012), privacy, communications, intellectual property infringement, trade on the Internet, taxation, consumer protection, advertising, censorship and freedom of speech related to the use of the Internet. It also protects websites, email, computers, cell phones, software, hardware and such other data storage devices.

Cyber law may also be called as Internet law as the area of law deals with the Internet's relationship to technological and electronic elements, including computers, software, and hardware and information systems. However, Cyber law includes the laws relating to crimes relating to Computers, Computer network, Internet, electronic devices, e-commerce or e-Business, cyber security, e-contract etc.

Categories of Cyber Crimes

Cyber crimes can be categorized based on as follows- (a) based on role of computer in cyber crime (b) based on perpetrators of cyber crime (c) based on victims of cyber crime (Nahar, 2011).

a) Categories Based on Role of Computer

Crimes in which the computer is target include offence as theft of intellectual property through unauthorized access to a computer can be physical or virtual. Besides, theft of marketing information or black mailing based on information gained from computerized files or data stored in it. Computer as a Tool means the crime could be

committed with the computer and computerization helps the criminals to commit crime faster. It includes fraudulent use of credit cards and account, conversation or transfer of account, theft of money accrual, telecommunication fraud etc (Nahar, 2011).

b) Categories Based on Perpetrators of Cyber Crime

It is divided into two types as *firstly*, Insiders and Outsiders; *secondly*, Hackers. Most of the cyber crimes are committed by the insiders like employees. Insider crimes include missing parts and software. Outsiders attack it to commit crime as outsiders. A hacker is a person seeking and stealing knowledge and distributing it with the world for profit or education and awareness or ill motive (Nahar, 2011).

c) Categories Based on Victims of Cyber Crimes

It is divided in five types as follows: 1. Crime against individual 2. Crime against organizations 3. Crime against economy 4. Crime against society. 5. Crime against national security (Nahar, 2011).

1. Crime against Individual

There are different types of crimes against individual, such as- (i) Identify theft, (ii) SMS spoofing, (iii) Hacking committed by hackers using (a) Telecommunication network or (b) Mobile network. (iv) Cyber stalking (v) Unauthorized use of ATM cards- Debit card, Credit card etc e.g. false ATM is used in order to do shopping or withdrawing money from the victim's bank account. (v) Cracking (vii) Unauthorized access to computer system. (viii) Illegal interception by technical means of non-public transmissions of computer data to, from or within a computer system (ix) Data interference i.e. unauthorized damaging, deletion, deterioration, alteration or suppression of computer data(x) Spamming (xi) Cheating and Fraud (xii) Harassment (xiii) Email-bombing (xiv) Indecent exposure and Dissemination of obscene material (xv) Defamation, violation of privacy (xvi) Drug trafficking (xvii) Spreading virus and worms (xviii) Intellectual property infringements (xix) Computer and network resources vandalism (xx) Forgery (xxi) Denial of services (DOS) (xxii) Salami attack (xxiii) Internet time and information theft/ Cyber theft which includes- embezzlement, DNS cache poisoning, Unlawful appropriation, Plagiarism, Piracy, Identify theft, stealing information, Money and other valuables (Nahar, 2011).

2. Crime against Organizations

(i) DOS (ii) Unauthorized control/access over the network resources and Websites (iii) Exposing obscene materials over the web pages (iv) Virus attack (v) E-mail bombing to organizations (vi) Salami attack (vii) Logic bomb (viii) Trojan horse (ix) Data diddling (x) Vandalizing the infrastructure of the network (xi) Blocking (xii) Theft of important possessions (xiii) Terrorism against government organizations (xiv) Tempest attack (Uddin et al., 2010). (xv) Web jacking; it occurs when someone vehemently takes control of website by cracking the password (Ahmed, 2012).

3. Crime against Economy

The following are the crime against economy- (i) Hacking (ii) Cracking. (iii) Phreaking (iv) Malicious programs include virus, worms, logic Bomb, Trojan horse and Hoax (v) Computer fraud (vi) Computer forgery and counterfeiting (vii) Theft of telecommunication services (viii) Intellectual property rights infringement (ix) Tax evasion (x) Computer sabotage (damaging the computer). Computer sabotage is of two types (a) Hardware sabotage and (b) Software sabotage. Software sabotage includes (i) Carding (ii) Packet sniffing (iii) Internet time theft denotes the usage by an unauthorized persons of the Internet hours paid by any persons (Ahmed, 2012).

4. Crime against Society

There are different type of crimes against Society i.e. (i) Porno Mailing, (ii) Social citing; it includes racial hatred and blasphemy. In this Crime wrongful use of social cites is done in order to spread enmity and feelings of hatred. (iii) Child pornography. (iv) Any hate propaganda (v) Forgery (vi) Online gambling (vii) Trafficking (viii) Financial crimes (ix) Indecent exposure (x) Web jacking. (xi) e-threatening (Nahar, 2011).

5. Crime against Government or National Security

The cyber crimes which affect the national security are (i) Cyber Warfare: Most of the Armies world over now has dedicated cyber warfare teams for defensive as well as offensive operations. (ii) Cyber Terrorism: Cyber terrorism means unlawful attacks and threats of attack against the computer, network and the information stored therein. Cyber terrorist attacks on the Internet of many academics, government and intelligence official's sites etc. (Nahar, 2011).

Reasons for Cyber Crime

The concept of Law has said human beings are vulnerable to crime so rule of law is required to protect them. Applying this to the cyberspace, we may say that computers are also vulnerable to crime so rule of law is required to protect and safeguard them. The reasons for the vulnerability of computers and high tech crimes may be said to be for the certain reasons (Nahar, 2011) as- (a) Capacity to store data in comparatively small space, (b) Easy to access to codes, advanced voice recorders, retina imagers etc. (c) Complex computer operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas. (d) Negligence in protecting the computer system in turn provides cyber criminals to gain access and control over the computer system (Patil, 2014) (e) Hactivists on game competition commits cyber crime like hacking, DDOS etc. (Bdnews24.com, 2015) (f) Loss of evidence is a very common & obvious problem as all the data are routinely destroyed and criminals are encouraged. Thus cyber crimes go on increasing day by day and its scope also increasing in the same way (Rashid, 2009).

State of Cyber Crime and the Status of Legal Mechanism in Bangladesh

State of Cyber Crime

The use of Internet started in Bangladesh in 1993 for the first time (Ahmed, 2014). It was opened for all on June 4, 1996 through the commissioning of VSAT (Very Small Aperture Terminal) connection but this introduction could not create a good market at the very initial stage (Rashid, 2009). After the year 1996, there were only two ISPs (Internet Service Providers) and about one thousand of users in the country. But owing to the rapid growth of this industry 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 Telecommunication Company Limited (BTCL) and Bangladesh Telecommunication Regulatory Commission (BTRC) reduced the bandwidth price at regular intervals which attracted more and more users towards the Internet world. As of now BTRC (2014) has counted about three hundred and forty five plus registered ISP license holders.

The present government has 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 using IT sectors. But the Government as well as other concerns consider cyber crimes worriedly that are being committed in this virtual world with the expansion of Internet and other networks which owes to convert this country into a digital country.

In Bangladesh, cybercrime has drawn public attention for the last couple of years. On August 23, 2004, an email was sent to a Bangla daily threatening to kill Sheikh Hasina, the supreme leader of a major political party. After two days, on August 25, 2004, another email was sent to the Bangladesh police Headquarters issuing threat to Khaleda Zia, supreme leader of another major political party, her elder son and some members of parliament (Current Affairs, 2014). It is difficult for most isolated users of Information Technology (IT) to understand the term 'Cyber crime'; Bangladesh is no exception. Here cyber crimes started with spam mails and trojan attack. Cyber crime is increasing in Bangladesh day by day. Cybercrimes take place in Bangladesh mainly in the following sectors: (a) Cybercrime against individuals; (b) Cybercrime against property and financial institutions; (c) Cybercrime against organizations; (d) Cybercrime against society; and (e) Cyber crime against national security.

In the year of 2013, the Skype conversation and blogging were the burning issues of our country. Pornography video and picture upload happen in our country on a regular basis (Current Affairs, 2014). Besides, blackmailing girl by capturing their nude photographs is caused frequently by their boyfriends and others. 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. Hacking committed into the Internet account of Barisal DC office in 2003, the incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Telegraph and Telephone Board (BTTB). Hacking took place in the website of Bangladesh Rapid Action Battalion (RAB) in 2008, when Hackers accessed to www.rab.gov.bd, the website read: "Hacked by Shahee_Mirza." (*The Daily Star*, 2008), Hacking committed into the mail of BRAC Bangladesh (Borhanuddin, 2006), the transaction report of Dhaka Stock Exchange has been stolen through hacking ; crime committed through inserting naked pictures to the website of Bangladesh National Parliament, inserting naked pictures to the website of Jamate Islami Bangladesh, inserting naked pictures to the website of the Daily *Jugantor*, E-mail threatening to World Bank Dhaka Office and involvement in cyber warfare with India etc (Borhanuddin, 2006). Besides most recently in 2014 and 2016,

stealing money from Sonali Bank by hacking password and Bangladesh Bank heist remembers the ferocity of cyber crime in Bangladesh.

Before 2013, there was cyber tribunal only theoretically not practically in Bangladesh. So in that period cyber crimes were tried by the session courts. After passing the ICT Act in 2006, a few number of cases found to be filed. In the recent days, a lot of cases are being filed. Some of them are- (i) Four Bloger's case: four bloggers of Bangladesh namely Asif Mohiuddin, Subrata Adhikari Shovu, Rasel Parvej and Moshiur Rahman Biplob were charged on 27th June, 2013 under sect 57 of the ICT act for writing ill statement about Islamic religion and prime minister in the facebook and Blogs. (ii) Adilur Rahman Khan's case: Adilur Rahman Khan, Director of "*ADHIKAR*" (Non Government Human Rights Organization), was charged U/S 57 (1), (2) of the ICT Act, 2006 and U/S 500 (c) and (d) of the Penal Code,1860 on 4th September, 2013 for publishing report of 5th may of *Hefajat* movement at *Shapla Chattar, Matijhil*, alleged that the number of dead body reported by "*Adhikar*" is 60 (sixty), was false and intended to degrade the reputation of the Govt, to instigatie the muslims, to hamper the reputation of the State to the foreign states. (iii) Mahmudur Rahman Khan's case: the editor Mahmudur Rahman Khan and Publisher Hasmat Ali of the daily newspaper "*Amar Desh*" were charged U/S 56 and 57 of the ICT Act, 2006 and sections 124, 124 (a), 505 (a), 120 (b) and 511 of the Penal Code ,1860 for publishing the Skype conversation between justice Nijamul Haque Nasim (the then Chairman of International War Crimes Tribunal-1) and his Belgium friend Dr. Ahmed Jia uddin on 13th December, 2012 (Ahmed, 2014). Thus cyber crime is the main concerning issue of Bangladesh government today.

Status of Legal Mechanism

National legislative frameworks

The United Nations Commission on Internet Trade Law (UNCITRAL) adopted as the Model Law on Electronic Commerce in 1996. The Model Law provides that all Nations should give consideration to it when they enact and revise their cyber laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Hence the enactments of Bangladesh in this regard are the National ICT Policy-2009, preparing Information Technology (Electronic Transactions) Act (ITETA), 2000. It is to be noted here that ITETA seems to be a close replica of the Indian IT Act-2000 that failed to include issues like cyber squatting, spam and cyber terrorism. The Information and

Communication Technology (ICT) 2006 has been enacted based on the said Model Law and come into force on 8th October-2006 and ICT rules in 2010 to facilitate electronic commerce and encourage growth and development of information technology. It includes the provisions of bringing the cyber criminals within the ambit of criminal jurisdiction (Reza & Azim, 2009). The ICT Act was amended in 2013. This Act not only extends to the whole of Bangladesh but also applies to offences and contraventions committed outside Bangladesh (Sec.4 of the ICT Act, 2006). It has 90 sections divided into 10 chapters. 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 probable cases and grounds and give penalty for cyber crimes frequently occurring at present and which might occur in future. Some major questions are raised regarding the distinctive nature of committing cyber crime and as to no treating cyber crime and cyber civil wrong separately. Recently, Digital Security Act, 2016 as a supplemental to the ICT Act, 2006 is adopted by the Cabinet which expected to make a strong legal framework to combat cyber crime in Bangladesh. This act has 45 sections divided into seven chapters which empower Government to establish National Digital Security Agency (NDSA) headed by a Director General. With a view to securing, preventing and curbing cyber criminal activities, NDSA is authorized to monitor, observe and take necessary steps in respect of all the Bangladeshi computers or digital systems, networks, mobiles or digital communication (voice and data) networks etc. NDSA for this purpose can establish digital forensic lab for cyber forensic analysis and it can also establish Bangladesh Cyber Emergency Response Team (Bangladesh-CERT) for quick response against cyber crimes (Section 5 of the Digital Security Act, 2016). Besides, there will be a National Digital Security Council (NDSC) chaired by the prime minister to talk about cyber related issues and take immediate decisions (Section 6 of the Digital security Act,2016). This Act also makes all the provisions of the Reciprocal Co-operation Act 2012 applicable to investigate, prosecute and adjudicate the trans- broader offences in the question of regional and international cooperation (Section 39 of the Digital security Act, 2016) and all the Offences committed under this act have been made triable under the cyber tribunal and cyber appellate tribunal established under the ICT Act, 2006.

Bangladesh Government has set up a special tribunal under the ICT Act, 2006 called 'Cyber Tribunal' at Dhaka in 2013 to handle

cybercrimes that include fraudulence, extortion and the hacking of computer system on-line. The move came after the UK-based Economist claimed that it had recorded 17 hour conversation on Skype and 230 emails between the 'International War Crimes Tribunal 1' Chairman and Bangladeshi expatriate in Brussels. The 'International War Crimes Tribunal 1' Chairman, Justice Md. Nizamul Haque, resigned his position amid controversies over his conversation with the expatriate Ahmed Ziauddin (Bangladesh Shangbad Shangstha, 2013).

The law ministry issued a gazette notification on the establishment of the tribunal on January 28, 2013 under the Information and Communications Technology Act 2006 in Dhaka to exclusively deal on-line crimes in a speedy manner. Initially, one tribunal was set up in Dhaka covering the whole of Bangladesh although the law stipulates that one or more cyber tribunals could be set up for an effective and speedy trial of criminal activities committed on-line (Bangladesh Shangbad Shangstha, 2013). Cyber Tribunal, the first of its kind in the country, will be empowered to conclude trials within six months. Several hundred of complaints have been filed before this tribunal and the trial of those are in pending.

Provisions for setting up cyber tribunal and cyber appellate tribunal having original and appellate jurisdiction respectively and punishments of lighter/severe form, trial procedure etc have been provided by the ICT Act, 2006 (Sec. 82 & 84 of the ICT Act, 2006). But it is worth-mentioning here that the ICT Act, 2006 is not exhaustive enough to protect this gigantic cyber space and IT industry. In addition to the application of the provisions of the ICT Act, a good number of procedural and structural hurdles are being faced which are as follows:

Lack of Technical Expert: Judges and the lawyers of cyber tribunal or session Courts (Sec. 68 (2) of the ICT Act, 2006) are the experts of laws, not of technology, more specifically of Internet technology. So the judges of cyber tribunal as well as cyber appellate tribunal (Sec. 82 of the ICT Act, 2006) 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 the Act is that so far no provisions exist taking initiative by the Government to train up the judges for acquiring the minimum technological knowledge required for ensuring justice. The Digital Security Act, 2016 also failed to emphasize on this issue.

Lack of Knowledgeable law enforcers: A police officer not below the rank of a Sub-Inspector can be the IO i.e. Investigation Officer regarding the cyber crimes (Sec. 69 of the ICT Act, 2006). Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of cyber tribunal and cyber appellate tribunal. So, is it possible for such a police officer to make a proper investigation into such matters? Moreover, it may result in a snag to justice. (Uddin et al., 2010)

Procedural Difficulties: The Government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of the tribunals (Sec. 82 of the ICT Act, 2006) .Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state in this regard. (Uddin et al., 2010)

Lack of Clearance of the Terms: The cyber crime related terms have not been defined in this Act such as data diddling, tempest attack etc. for which existing law suffers from proper application.

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

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

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

Regional Strategies and the Status of Cyber Law

Cyber law covers a wide diversity of political and legal issues related to the Internet and other communication technology protecting intellectual property, privacy, freedom of expression in one's jurisdiction. It also examines the cyber related laws of SAARC countries, USA, Australia, Japan, and European and similar legislations. Overseas regional countries around the world are promoting international measures to deal appropriately with cyber crime for the growth of telecommunications, computer network. One of them is the Hyderabad Declaration (2004) which declares that harmonizing the legal and administrative framework for developing trust in e-commerce transactions across Asian countries. Based on UNCITRAL Model Law (1996), Neighbouring country India enacted many cyber related laws, rules and regulations for protection ICT development parallel with other sectors. The Indian Information Technology (ITA) Act-2000 was the first step towards information technology security in the country and strives to improve the concept of electronic governance and e-commerce. The Indian Parliament received the Semiconductor Integrated Circuits Layout-Design (SICLD) Act, 2000 after the assent of the President on the 4 September 2000 and the other IPR Act i.e. The Patent Act, Trade Marks Act, Copyright Act etc.

Cyber related or cyber crime legislations are still unhappily absent in Africa, the Middle East, Asia and Oceania. Technologically and highly developed countries, especially those in Europe and North America have cyber related laws and cyber crime laws to protect and save their privacy, computer, computer network and Internet. Some developing countries are now taking initiatives in this respect.

Global Strategies and the Status of Cyber Law

International law, conventions, bilateral and multilateral treaties have not been developed for Internet filtering and governing the cyber crime. The European Convention on Cyber Crime came into force in 2001. The European Convention on Cyber Crime, 2001 is the first ever-international treaty on criminal offences committed against or with the help of computer networks such as the Internet. After United Nations protocol on cyber security and cybercrime, The United Nations Office on Drugs and Crime (UNODC) has published a practical guide. The guideline emphasizes on the use of the Internet for terrorist purposes among member states for more effective investigation and prosecution of terrorist cases involving the use of the Internet. Powerful countries including USA, Britain,

China, Russia, Philippine and many of the countries are thinking and preparing law to protect the cybercrimes.

International Laws & Conventions on Cyber Law: International law provides few obvious tools to analyze Internet filtering, through the potential surety exists (The United Nations Convention on the Use of Electronic Communications in International Contracts, 2005). Countries often make law through multilateral agreements that bear on Internet law and regulation. For instance, trade agreements frequently include provisions related to intellectual property that could affect filtering issues. A next generation of international humanitarian law, some have argued, might also include protections for access to communications.

The European Convention on Cyber Crime-2001: The European Convention on Cyber Crime-2001 is the first ever international treaty on criminal offences committed against or with the help of computer networks such as the internet. The Ministers of Foreign Affairs finally adopted the Convention on November 8, 2001. The Convention on cyber crime was opened for signature in Budapest, Hungary on November 23, 2001. Ministers or their representatives from the 26 fellow Member States signed the treaty. The total number of signatories is 43. By signing this treaty, member countries agreed on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals (Nair, 2013).

Other International Strategies: Some of the international organizations have realised and recognized trans-border nature of cybercrime and the need for international harmonization of technical, legal and other solutions (Chawki, 2005). The main of them in this field are the Organization for Economic Cooperation and Development (OECD), the Council of Europe, the European Union, G-8 and the Interpol. In addition, the UN, World Intellectual Property Organization (WIPO) and General Agreements on Trade and Tarrifs (GATS) have also played an important role. These organisations have significantly contributed to the harmonisation of criminal law as well as of civil and administrative law in all of the areas of computer-related law reform. The first comprehensive inquiry into the penal law problems of computer related crimes on international level was initiated by the OECD. The OECD carried out from 1983 to 1985, a study of the possibility of an international harmonization of criminal laws to address computer related crimes (United Nations Manuel on the Prevention and Control of Computer Related Crime, 1995). The study reported in 1986, on surveying

existing laws and proposals for reform and recommended a minimum list of abuses, that countries should consider penalizing by criminal law.

From 1985 until 1989, the selected Committee of Experts on Computer Related Crime of the Council of Europe discussed the issues raised by cybercrime and drafted recommendation, which was adopted on September 13, 1989. This recommendation emphasized on the importance of an adequate and quick response to the newly encountered challenge of cybercrime. In the guidelines of national legislatures to review and enhance their laws, the Recommendation featured a 'minimum list' of necessary candidates of such crimes to be prohibited and prosecuted by international consensus, as well as an optional list that describes prominent offences on which international consensus would be difficult to reach.

In 1990, the English United Nations Congress on the Prevention of Crime and Treatment of Offenders addressed the legal problems posed by cybercrime. It produced a resolution which called for Member States to intensify their efforts to combat computer-related crimes by modernizing their national legislations, improving security measures and promoting the development of comprehensive international framework of guidelines and standards for prosecuting these crimes in the future(8th UN Congres, 1990). Two year later, the Council of the OECD and 24 of its Member countries adopted a Recommendation of the Council concerning guidelines for the Security of information system intended to provide a foundational information security framework for the public and private sectors (OECD, 1992). The Guidelines for the Security of Information Systems were annexed to the Recommendation. This framework includes codes of conduct, laws and technical measures. They focus on the implementation of minimum standards for the security of information systems. However, these Guidelines request that Member States establish adequate penal, administrative of other sanctions for misuse and abuse of information systems.

In 1995, the UN published the United Nations Manual on the Prevention and Control of Computer Related Crime (Chawki, 2005). This Manual studied the phenomenon of computer-related crimes, substantive criminal law protecting privacy, procedural law, and the needs and avenues for international cooperation (UN Manual, 1995). In the same year, the Interpol organised its first Conference on Computer Crime. This conference confirmed that a high level of concern existed in the law enforcement community over the

propagation of computer crime. Later on, Interpol held several conferences on the same theme. In the same year also, the Council of Europe adopted Recommendation of the Committee of Ministers to Member states, spelling out the principles that should guide states and their investigating authorities in the domain of IT (the Council of Europe Recommendation, 1995). Some of these principles cover search and seizure, obligation to co-operate with investigating authorities, the use of encryption and international co-operation (Goodman & Brenner, 2002).

On April 24, 1997, the European Commission (Walker & Akdeniz, 1998) adopted a resolution on the European Commission's communication on illegal and harmful content on the Internet, supporting the initiatives undertaken by the Commission and stressing the need for international co-operation in various areas, to be initiated by the Commission. One year later, the European Commission presented the European Council with a report on computer-related crime it had contracted for.

Some years later, the Council of Europe's Committee of Experts on Crime in Cyber-Space took his assignment to heart, preparing a Draft Convention on Cybercrime. The preparation of this Convention was a long process; it took four years and twenty-seven drafts before the final version, dated, May 25, 2001 was submitted to the European Committee on Crime Problems at its 50th Plenary Session, held on June 18-22, 2001 (Goodman & Brenner, 2002). Chapter II of this Convention contains the provisions that are relevant to the issues under consideration in this article. This Chapter is divided into two sections: Section 1 deals with 'substantive criminal law'; Section 2 deals with 'procedural law'. According to the Explanatory Memorandum accompanying the Draft Convention, Section-1 seeks 'to improve the means to prevent and suppress computer-or computer related crime by establishing a common minimum standard of relevant offences' (Uddin et al., 2010).

Parties to the Convention would agree to adopt such legislative and other measures as may be necessary to establish certain activities of cybercrimes under their 'domestic law'. According to Section 1 of Chapter II of the Convention, these activities are: (1) Offences against the confidentiality, integrity and availability of computer data and systems; (2) Computer-related offences; (3) Child pornography; (4) Offences related to infringements of copyright and related rights; (5) provisions governing the imposition of aiding and abetting and corporate liability.

From their part, the G8, held in May of 2000 a cybercrime conference to discuss how to jointly crack down on cybercrime. This conference brought together about 300 judges, police, diplomats and business leaders from the G8 states. It drafted an agenda for a follow-up summit to be held in July (Goodman & Barner, 2002). At the July, 2000 summit, the G-8 issued a communication which declared, in pertinent part, that it would take a concerted approach to high-tech crime, such as cybercrime, which could seriously threaten security in the global information society. The communication noted that the G8 approach to these matters was set out in an accompanying document, the OKINAWA Charter on Global Information Society (Rossudowska & Barker, 2011).

Cyber Related Laws in Other Developed Countries

Technologically highly developed countries, especially those in Europe and North America , Australia, South Korea, Singapore, Japan have cyber related laws and cyber crime laws to protect and save their privacy, computer, computer network and Internet. Some South American countries have cyber laws that prevent some categories of cyber crime, but others have essentially no cyber laws in place. Administrative, penal and civil legislation was enacted to protect data against illegal access to computer system and associated citizens' rights to privacy. The following countries enacted their cyber laws; Sweden in 1973 and 1986; the United States of America in 1974, 1980 and 1984; Denmark in 1978 and 1985; Austria in 1978 and 1987; France in 1977 and 1988; Japan in 1997 and 1988; Spain in 1992 and 1995; Italy in 1978 and 1997; Greece in 1988 and 1997; and Malaysia in 1997; etc (Ahmed, 2012). U.K., USA, India, Malaysia and some other developed countries have established special wings of police to combat the cyber crime. On the last 23rd July of 2009, North Korea twisted Korea Internet and Security agency, 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 (Uddin et al., 2010).

Defensive Measures of Cybercrime

Defensive measures must be taken in line with the legal steps in curbing cyber crimes. It is always better to take certain precaution while operating the Internet. A person should keep in mind the following things (Patil, 2014).

1. To prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friend as there have been incidents of misuse of the photographs.
3. Always use latest and update antivirus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
5. Never send your credit card number to any site that is not secured to guard against frauds.
6. Always keep a watch on the site that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security program that gives control over the cookies and send information back to the sites as leaving the cookies unguarded might prove fatal.
8. Web site owners should watch traffic and check any irregular activities on the site. This may be done by putting host-based intrusion detection devices on servers.
9. Use of firewalls may be beneficial in the protection of Cyber crime.
10. Web servers running public sites must be protected separately from internal corporate network.
11. Hackers hack our personal information by using our account ID and password such as our bank, e-mail ID and password. So the best way to protect us by using very strong password, we should never share our ID and password with other person and never write down our password elsewhere.
12. Before using any computers please make sure your computer is secured. We can secure our computer by using strong firewall software. Firewall is a very strong cyber defense software.
13. Use anti-virus software or programs. Before installing any programs please make sure this is secured and trusted site.

14. We should install the latest operating system.
15. We should never share our personal on-line account information with unknown person.

Recommendations

The following steps should be taken to prevent cybercrime in Bangladesh:

1. Clear and self-explanatory standard operating procedure to be imposed immediately for the Cybercrime Unit.
2. A comprehensive induction programs should be developed for all the concerns of ICT as pilot basis.
3. A separate Cybercrime Protection Act should be enacted.
4. Further there is a dire need for evolving a code of ethics on the cyber-space and discipline.
5. There must be clear operating procedure for cybercafé and voice over Internet protocol (VOIP) in Bangladesh. Bangladesh is a country of constitutional supremacy. Constitutional Safeguard against cyber crimes may escort the Cyber warfare to a national temperament.
6. Special trained wing of police to combat cyber crime should be established. The rise of cyber crime insists the law enforcers to work as global police rather than regional or national police only.
7. Cyber crime units can be established. Bearing in mind the present situation of using Internet and increasing cyber crime in Bangladesh, Government can also commence such types of agencies. The significance of such Units 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.
8. Observe Group should be established. These groups can be one of the vital constituents for developing Bangladesh as an advanced country especially in Internet technology.
9. Public Awareness should be strongly created. This course is not 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 cure 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.

Conclusion

Prevention is always better than cure**.** Cyber crime is increasing day by day. As a result we can be a victim of any cyber attack at any time. We should take precautionary measures as well as punitive measures against cybercrime. To make it fruitful, the Legislature, the Ministry of Information Technology along with the IT professionals and the media must work together. The young generation must be conscious about cybercrime. Apart from monitoring and controlling cybercrimes, Bangladesh Computer Security Incident Response Team (BD-CSIRT) should take punitive measures against the offenders and in some cases BD-CSIRT should take action directly against those who engage in carrying out harmful activities against students, society, state, political and religious beliefs using phone, Computer and other collateral devices . The Digital Security Act, 2016 strengthens the hand of Bangladesh-CERT to take emergency action against cyber criminal activities. Besides National Digital Security Agency (NDSA), National Digital Security Council (NDSC)'s formation, regional and international initiatives make us optimistic as the Bangladesh cyber space a safe zone of communication in the coming days.

References

Ahmed, Z. (2012) *A Text Book on Cyber Law in Bangladesh*, National Law Book Company, Dhaka.

Ahmed. D. Z. (2014) *Bangladesher Cyber Ain Totto o Bishleshion* (Bangla), Muhit Publications, Dhaka.

Agence France Presse (2012) 'Bangladesh war crimes chief judge resigns over hacked calls', dawn.com, viewed 11 April 2013.

Bdnews24.com (28.01.2015) front page, viewed 3 February 2015, available at http:// www.bdnws24. com/paper-edition/frontpage/129

Borhanuddin, A. R. M. (2006) *Cyber Crime and Bangladesh Perspective*, viewed 6 September 2009, available at http://www.scribd.com/doc/3399476/cyber-crime

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

Chawki, M. (2005) 'A critical look at the regulation of cybercrime a comparative analysis with suggestions for legal policy' *Journal for Information, Law and Technology* (JILT), viewed 10 October 2015, available at www.ie-ei.eu/.../criticallookatthe

Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states (1995).

Council of Europe (1989), Recommendation no. 4(89) 9 of the Committee of Ministers to Member States on Computer-Related Crime.

Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states (1995).

Current Affairs (2014) Dhaka, March, 2014, p. 23

Daily Star (Sunday, July 13, 2009) pp. 6-9, viewed 10 October 2009, available at www.thedailystar.net

Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders, Doc. A/CONF.144/L.11 of 4 September 1990 section 2.

Garner, B. A. (2004) *Black's Law Dictionary*, 8th edn, West Publishing Co., United States.

Goodman, M. D., Brenner, S. (2002) 'The emerging consensus on criminal conduct in cyberspace' *UCLA Journal of Law and Technology*, viewed 10 December 2014, https://archive.org/.../the *emerg*

Hackerman, N. & Robert, A. (1991) 'Computers at risk: safe computing in the information age' *National Research Council*, Welch Foundation, United Kingdom, viewed 10 February 2015, http:// www.nap.edu/openbook.php

Hornby, N. S. (2010) *Oxford Advanced Learner's Dictionary*, 6th edn, Oxford University press, UK.

'International crimes tribunal chairman resigns over skype', *Bangladesh Sangbad Sangstha* (BSS) (2013*)* National News Agency, 11 December 2012, retrieved 11 April 2013.

Janssen, C. (2012) *Techopedia Online Dictionary*, available at www.techopedia. *com/definition*, viewed 2 January 2015.

Nagpal, R. (2009) *What is Cyber Crime*, viewed 10 December 2014, http://issuu.com/rohas/does/ece.

Nahar, D. N. (2011) *Fundamentals of Cyber Law*, 1st edn, Bangladesh Law Book Company, Banglabazar, Dhaka-1100.

Nair, V.V. (2013) 'Dark deeds remain in the dark', *Financial Daily, a*vailable at http://www.thehindubusinessline.com/bline/ew/2003/09/10/index.htm

OECD Recommendation of the Council Concerning Guidelines for the Security of Information Systems (1992).

Patil, P. (2014) *Cyber Crime,* available at http://www.mavi.org/pati/pati: cybercrimes dec03html, accessed on12-11-2014.

Rashid, H. (2009) *Internet History of Bangladesh*, viewed 1 January 2009, available at http:// eziniearticles.com/? Internet-Historyof-Bangladesh&id= 2327010

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

Rossudowska, A. & Barker, J. (2011) 'An overview of the Okinawa Charter on the global information society and the DOT force – with a focus on Africa,' *Faculty of IT*, Bond University, Queensland, Australia.

Singha, J. Y. (2005) *Cyber Laws*, Universal Law Publishing Co. Pvt Ltd, India.

Sec.4, 68(2), 69, 82, 84 of the Information and Communication Technology Act (2006).

The Digital Security Act (Adopted by cabinet, 2016).

The Hyderabad Declaration (2004).

The UNCITRAL model law on electronic commerce (1996).

The Indian Information technology Act (2000).

The Semiconductor Integrated Circuits Layout-Design (SICLD) Act, (2000).

The United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

Udddin, A., Maruf M., Rabiul, M. & Ahamed, B. (2010) 'Emerging cyber threats in Bangladesh: in quest of effective legal remedies' *The Northern University Journal of Law*, Dhaka, vol. I, pp. 3-5.

United Nations Manuel on the Prevention and Control of Computer Related Crime (1995).

Walker, C. & Akdeniz, Y. (1998) 'The governance of the Internet in Europe with special reference to illegal and harmful content', *Criminal Law Review, Crime, Criminal Justice and the Internet*, Cyber Law Research Unit, Centre for Criminal Justice Studies, Department of Law, University of Leeds, available at www.cyber-rights.org/.../CrimLR_ya_98.pdf

Weimann, G. (2004) 'Cyber terrorism how real is the threat, special report', *United States Institute of Peace,* Washington, viewed 10 October 2015, http:www.usip.org/sites/.../sr119.pdf