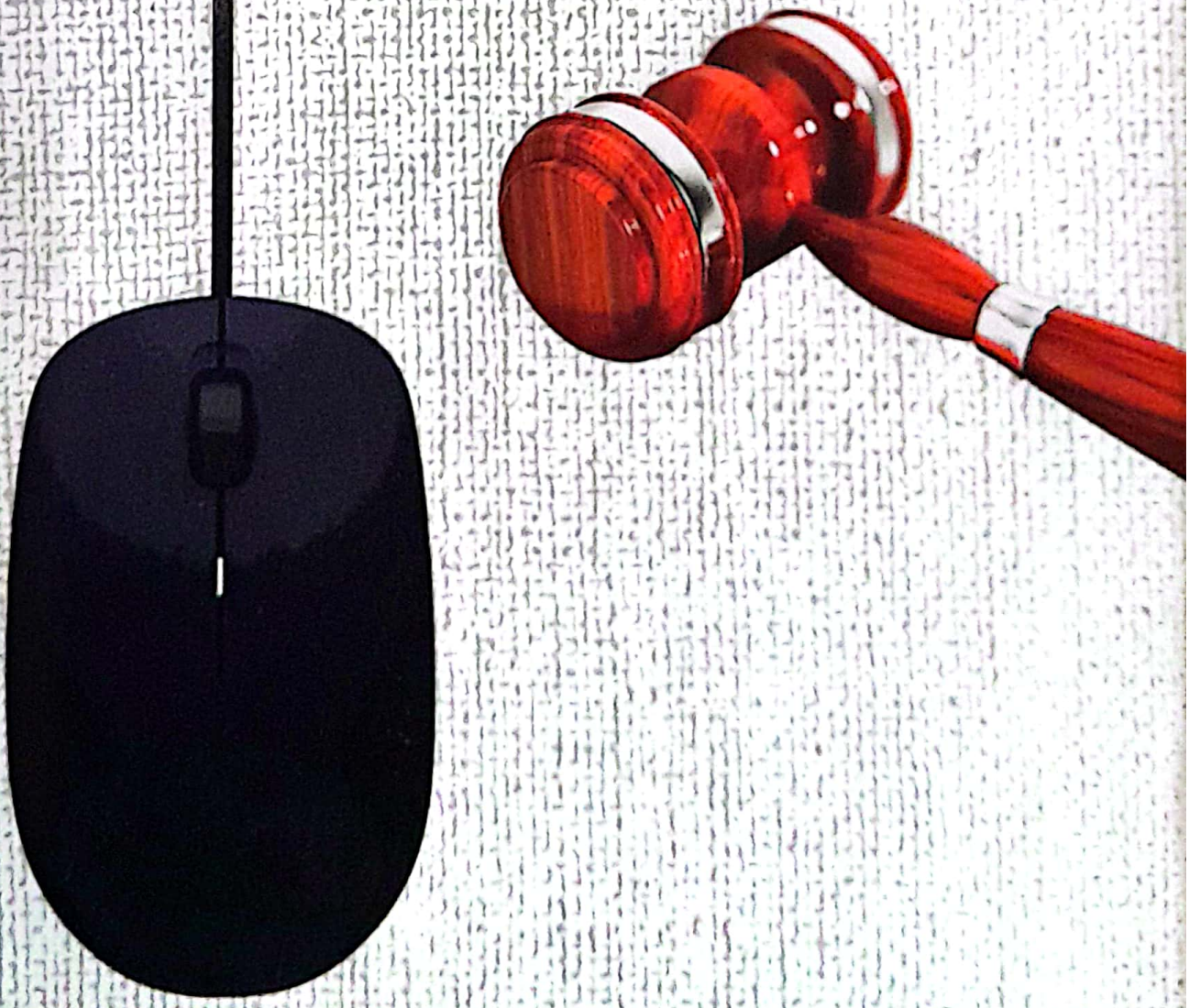
TEXTBOOK ON MEDIA AND CYBER LAW

Dr. Md. Raziur Rahman



Textbook on Media and Cyber Law

DR. MD. RAZIUR RAHMAN
Ph.D. (IU)
LL.M. (Coventry University, England)
PGDIP (UOG, England)
LL.M., LL.B. (Hon's) First Class First (IU)

Associate Professor & Dean
Faculty of Law
Bangabandhu Sheikh Mujibur Rahman Science and Technology University
Gopalganj-8100

BEACON PUBLICATIONS
Dhaka-Chattogram

ABBREVIATIONS

ADP	Automated Data Processing
ANSIR	Awareness of National Security Issues and Response
ANAO	Australian National Audit Office
AoI	Assurance of Information
ASDSC	Australian Strategic and Defence Studies Centre
ASIM	Automated Security Incident Measurement
ASP	Application Service Provider
ATM	Automated Teller Machine
BCC	Bangladesh Computer Council
BCS	Bangladesh Computer Samity
BIT	Bangladesh Institute of Technology
BSOSN	Bangladesh Open Source Network
BTTB	Bangladesh Telegraph and Telephone Board
BTRC	Bangladesh Telecommunication Regulatory Committee
CA	Civil Affairs
CAN	Computer Area Network
CMC	Computer Mediated Communication
CD	Computer Disk
CCM	Communication Counter Measures
CCU	Computer Crime Unit
CI	Counter Intelligence
CHIP	Computer Hacking and Intellectual Property
CIRC	Computer Incident Response Centre
CIS	Communications and Information System
CITAC	Computer Investigation and Infrastructure Threat Assessment Centre
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploit

CNI	Critical National Infrastructure
COMINT	Communications Intelligence
COMPUSEC	Computer systems security
COMSAT	Communications satellite
COMSEC	Communications Security
Con Ops	Concept of Operations
COP	Common Operational Picture
CSTARC	Cyber Security Tracking, Analysis & Response Centre
CTV	Community Television
DAB	Digital Audio Broadcast
DARPA	Defence Advanced Research Projects Agency
DASD	Deputy Assistant Secretary Department
DBS	Digital Broadcasting System
DCFL	Defence Computer Forensic Laboratory
DOS	Disc Operating System
D DoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DMCA	Digital Millennium Copy Right Act
DSL	Digital Subscriber Line
EA	EW - Electronic Attack
EC	Electronic Combat
EC	Electronic Commerce
EDI	Electronic Data Interchange
ECCM	Electronic Counter-Counter Measures
ECM	Electronic Counter Measures
EFT	Electronic Funds Transfer
EEI	Essential Elements of Information
EIIP	Energy Infrastructure Interdependencies Program
EIW	Economical Information Warfare
ELINT	Electronic Intelligence
EM	Emergency Management
EMP	Electromagnetic Pulse
ENISA	European Network and Information Security Agency
EO	Executive Order
EO/IRCM	Electro-optical/Infrared Counter Measures
EP	Electronic Protection

EPM	Electronic Protection Measures
ES	EW - Electronic Support
GATT	General Agreement on Tariff and Trade
FTP	File Transfer Protocol
FM	Frequency Modulation
GII	Global Information Infrastructure
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HackInt	Hackers Intelligence
HEL	High Energy Laser
HEMP	High-altitude Electromagnetic Pulse
HERF	High Energy (Emission) Radio Frequency
HF	High Frequency
HNA	Human Network Attack
HTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
HUMINT	Human Intelligence
ICT	Information and Communication Technology
ID	Information Dominance
IDC	Information Dominance Centre
InfraGard	public-private partnership to protect critical infrastructures
Info Ops	Information Operations
IO	Information Operations (old abbreviation - abandoned because of conflict with International Organization)
IP	Internet Protocol
INFOSEC	Information systems security
IPB	Intelligence Preparation of the Battle space
IPIA	International Partnership for Information Assurance
IPTF	Infrastructure Protection Task Force
IRT	Incident Response Team
ISO	International Standard Organization
ISP	Internet Service Provider
ISPAB	Internet Service Provider Association of Bangladesh
IST	Information Systems Terrorism
IT	Information Technology

ITU	International Telecommunication Union
IW	Information Warfare
LAN	Local Area Network
LW	Long Wave
MAN	Metropolitan Area Network
MW	Medium Wave
MF	Medium Frequency
MMS	Multimedia Messaging Service
MTP	Mail Transfer Protocol
MoD	Ministry of Defence
MOOTW	Military Operations Other Than War
NCS	National Communication System
NCSD	National Cyber Security Division
NGO	Non-Government Organisation
NSP	Network Service Provider
NTP	National Telecommunication Policy
NTRC	National Telecom Regulatory Commission
OPSEC	Operations Security
OSCINT	Open Source Intelligence
OSS	Open Source Software
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
PSYOPS	Psychological (Warfare) Operations
PSYW	Psychological Warfare
RADINT	Radar Intelligence
RAM	Random Access Memory
RAS	Remote Access Server
SREMP	Source-region Electromagnetic Pulse
SW	Short Wave
TCP	Transmission Control Panel
TELINT	Telecommunications Intelligence
THEL	Tactical High Energy Laser
TIW	Transnational Infrastructure Warfare
TW	Technical warning
UNCITRAL	United Nations Commission on International Trade Law
UHF	Ultra High Frequency

UWB	Ultra-wideband
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol
WISP	Wireless Internet Service Provider
WMD	Weapons of Mass Destruction
WME	Weapons of Mass Effect
WWW	World Wide Web

CONTENTS

Chapter One
Cyber Crimes Preliminary

Chapter-Two
Cyber Jurisprudence and Jurisdiction of Cyber Law

Chapter Three
The Right to Freedom of Opinion and Expression under the Cyber Legislation in Bangladesh

Chapter Four
Internet Privacy

Chapter Five
E-commerce in Bangladesh

Chapter Six
E-Contract

The Law of Electronic Contracts in Bangladesh

Chapter Seven
E-learning

Chapter Eight
Prevention of Cyber Crimes

Chapter Nine
E-governance

Chapter Ten
Privacy Protection and Cyber Security

Chapter : Eleven
Right to Information Act 2009

CHAPTER ONE
Cyber Crimes Preliminary

1. Introduction

Human beings are growing more reliant on automation as a result of technological advancements. It has profound effects on all aspects of life and society. The history of automation started with Babbage's creation of the computer, and with the advent of networks, notably the Internet and World Wide Web, a new horizon was opened (WWW). In today's digitalized world, the internet has become the backbone of all types of communication systems, as well as one of the most significant sources of information. It is a network of networks[1] made up of millions of private and public, academic, commercial, and government networks that are connected via copper lines, fiber-optic cables, wireless connections, and other technologies. The World Wide Web is a massive collection of interconnected documents, pictures, and other resources linked together via hyperlinks and URLs.[2] The internet enables computer users to quickly connect to other computers and store data all around the globe. Depending on the needs, they may offer to do so with or without the use of security, authentication, and encryption

---

1. Peter Norton, Introduction to Computers, 5th edn, Career Education, USA, 2002, p. 23.
2. The term URL means "Uniform Resource Locator, internet address. It is the address of a web page. Each page has its own unique web address (URL). This is how your computer locates the web page that you are trying to find. An example of a URL is : http ://funbrain.com/index.html. In this example URL, funbrain.com is called the domain name. The "index.html" refers to the specific page.

technology. This unrestricted network access allows certain highly competent criminals to engage in unlawful activities in the cyber realm. Crashing a computer system, stealing information stored in electronic form; e-mail bombing, data tampering, financial fraud such as unauthorized money transfers by cracking credit card security codes, denial of service, and virus attacks are among the most frequent evil deeds. However, in our nation, the institutional and legal foundation for preventing and punishing these crimes is insufficient.

2. An Overview of Cyber Crimes

The terms 'cyber crime' 'computer crime' 'information technology crime' and 'high-tech crime' are often used interchangeably to refer to two major categories of offenses. Firstly; the computer is the target of the offence; attacks on network confidentiality, integrity and/or availability i.e. unauthorized access to and illicit hampering with systems, programs or data, all falling into this category.[3] Secondly; traditional offences such as theft, fraud, and forgery that are committed with the assistance of or by means of computers, computer networks and related information and communications technology; here, the computer is a tool used to commit a conventional crime.[4] Cyber crime is a criminal activity done using electronic devices, computers and the internet. The Council of Europe's Cyber Crime Treaty uses the term 'cyber crime' to refer to offences ranging from criminal activity against data to content and copyright infringement.[5]

A recent study noted, cyber crimes differ from terrestrial crimes in four ways : 'They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be

---

3. M. D. Goodman, 'Why the PoliceDon't Care about Computer Crime', 10 Harvard Journal of Law and Technology, vol.465, 1997, pp.468-469. http ://jolt.law.harvard.edu/articles/10hjolt465.html. See also Criminal Threats to E-Commerce 17, Interpol, Jan. 2001.
4. ibid.
5. T. Krone, High Tech Crime Brief, Australian Institute of Criminology, Canberra, Australia, 2005.

committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.'[6] They also pose far greater challenges for law enforcement. Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.[7]

Cyber crimes pose unique legal and political issues because it is usually international in nature. The issues to be so addressed are as follows :

i. There is no single international entity that can investigate and prosecute international cyber crimes.
ii. There is also no clear definition of cyber crime at the international level, so countries have different standards for defining various forms of cyber crimes such as violation of intellectual property rights, right to privacy and child pornography.
iii. There are different requirements for record keeping among various countries such as how long traffic logs need to be kept and legal ability maintained to monitor the perpetrator.
iv. The victim and perpetrator are found often in different countries complicating where the case should be prosecuted.
v. The evidence can also remain in multiple countries making its collection very difficult.

---

6. Cyber Crime and Punishment, Archaic Laws Threaten Global Information, Mcconnell International, Dec, 2000. Available at http :// www.mcconnellinternational /service/ cybercrime.htm.(accessed 3 April 2015)
7. ibid.

After analyzing the above issues it can be said that, the cyber crime is one kind of digital crime which occur by using computer, internet, mobile phones etc. It is a criminal activity or a crime that involves the internet, a computer system, or computer technology.

3. Brief History of Using Internet in Bangladesh

In late 1995, the Government of Bangladesh invited applications to subscribe the Very Small Aperture Terminal (VSAT)[8] data circuits and on June 4, 1996 the VSAT connection was commissioned and the internet was launched in Bangladesh for the first time. The first usage of internet was the publication of the National Polls Result in 1996.[9] But this introduction could not create a good market at the very initial stage. After the year 1996, there were only two Internet Service Providers[10] (ISPs) 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 180 ISPs were working by 2005. In 2006 Bangladesh got connected with Submarine Cable which afforded big bandwidth and low cost than ever before. After this, over the years Bangladesh Telecommunications Company Ltd. (BTCL), presently 'Bangladesh Telecommunication Regulatory Commission' (BTRC)[11], reduced the bandwidth price at regular intervals which

---

8. The term Very Small Aperture Terminal may be mentioned as VSAT throughout the study.
9. Hamidur Rashid, Internet History of Bangladesh, http ://ezinearticles.com/ ?Internet-Historyof-Bangladesh&id=2327010 (accessed 1 January 2015).
10. An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.
11. The Bangladesh Telecommunication Regulatory Commission (BTRC) is an independent commission founded under the Bangladesh Telecommunication Act, 2001 (Act no 18 of 2001). The BTRC is responsible for regulating all matters related to telecommunications (wire, cellular, satellite and cable) of Bangladesh.

attracted much more users to the internet world. As of now BTRC has about three hundred and forty five[12] registered ISP license holders[13] and there are approximately 4.5 million users connected to them which is about 0.32% of the total population of the country.

4. Cyber Crime Defined

It is a technological crime and a misnomer[14] 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 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 : (i) crimes that target computer networks or resources directly; and (ii) crimes facilitated by computer networks or devices. Examples of crimes that primarily target computer networks or devices include malware and malicious code, denial-of-service attacks and computing viruses. Examples of crimes that merely use computer networks or devices include, amongst others, cyber stalking, fraud and identity theft and information

---

12. Report on BTRC, ISP Natiowide-94, ISP Central Zone-79, ISP Zonal-53, ISP Category A-99, ISP Category B-16, ISP Category C-04.
13. Summary of- BTRC licenses, http//www.btr.gov.bd, (accessed 1June 2015).
14. A.R.M Borhanuddin, Cyber Crime and Bangladesh Perspective, Available Online: http ://www.scribd.com/doc/3399476/cyber-crime,(accessed September 2015).

warfare. The Cyber Crime is further subdivided into the following four categories :[15] (i) cyber crime against individuals, (ii) cyber crime against property, (iii) cyber crime against organization, and (iv) cyber crime against society at large. Such a crime can broadly be defined as criminal activities using information and communication technology including the followings, which can be committed against the above mentioned groups :

4.1. Cyber Crime against individuals

Hacking or Cracking, Illegal/Unauthorised access, Illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system),Data interference (unauthorized damaging, deletion, deterioration, alteration, or suppression of computer data),E-mail spoofing, Spamming, Cheating and Fraud, Harassment and Cyber stalking, In decedent exposure, Defamation, Drug trafficking, Transmitting virus and worms, Intellectual property crimes, Computer and network resources vandalism, Internet time and information thefts, Forgery, Denial of services, Dissemination of obscene material.

4.2. Cyber Crime against property

Credit card fraud, Intellectual property crimes, Internet time theft.

4.3. Cyber Crime against organizations

Unauthorised control/access over the network resources and websites, Exposing indecent/obscene materials over the web pages, Virus attack, E-mail bombing, Salami attack, Logic bomb, Trojan horse, Data diddling, Blocking from access, Theft of important possessions, Terrorism against government organizations, Vandalising the infrastructure of the network.

---

15. Classification of Cyber crime, Report Cyber crime, http ://www.reportcybercrime.com/case_study_details_user.php,(accessed 1 January 2015).

4.4. Cyber Crime against society

Forgery, Online gambling, Trafficking, Pornography (especially child pornography), Financial crimes, Polluting the youth through indecent exposure, Web jacking.

The crimes mentioned above may be defined briefly as follows :

(a) 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.

(b) 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 and hackers use it for discussing their exploits/sharing the techniques. Paedophiles use chat rooms to allure small children.

(c) Cyber Stalking : In order to harass a woman her telephone number is given to others as if she wants to be friends with males.

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

(e) Hacking : Hacking is a simple term which means illegal intrusion into a computer system without permission of the owner/user.

(f) Denial of Services : This is an act by a criminal who floods the bandwidth of the victim's network or fills 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.

(g) 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.

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

(i) Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the internet e. g. if someone publishes defamatory matters about someone on a website or sends e-mails containing defamatory information.

(j) 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.

(k) Salami Attack : When negligible amounts are removed and accumulated into something larger. These attacks are used for the commission of financial crimes. A 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 approaches the bank for such small amount but the criminal gains a huge amount.

(l) Intellectual Property Crimes : These include software piracy like illegal copying of programs, distribution of copies of software, and copyright infringement like trademark violations, stealing computer source code etc.

(m) 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.

(n) E-mail Bombing : This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

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.

(o) 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.

(p) Forgery : When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery.

(q) 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, and networks where information is stored.

(r) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political or monetary objectives.

5. Present Scenario of Cyber Crimes in Bangladesh

Bangladesh does not have enough natural resources and has been trying to gain economic development through the utilization of Information Communication and Technology industry. Over the last few years, many nations have taken the advantage of 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 overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development.[16] The present Government has also declared the vision-2021 *i.e.* within 2021 this country is desired to become Digital Country and the per capita income equal to that of a middle-income country. In such a situation the Government and other concerns should address the scopes of commission of criminal activities that may be take place in the country as well as rest of the world with the expansion of internet and other networks for the purpose of converting the country into a digital one.

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is

16. 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, (accessed 12April 2015).

thought to be the earliest form of a computer, has been in India, Japan and China since around 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. It 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 were under cyber attack and the attack was remarkably successful in limiting public access to victim websites such as government websites, treasury department, federal trade commission and secret service.[17] Information technology (IT) experts believe that about 90 per cent of cyber crimes remain unreported. In case of Bangladesh, the situation is getting worse day by day. The most common cyber attacks and crimes committed in Bangladesh are listed below :

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

ii. 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.

---

17. 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-wagedagainst-us-s-korean-gov-sites/, (accessed 22 April2015).

iii. Hacking in the website of Bangladesh Computer Society, which took place after a few days of a three day-long 'Regional Seminar on Cyber Crime' in Dhaka.[18]

iv. E-mail threatening the Prime Minister Sheikh Hasina from a cyber cafe.[19]

v. Hacking into the internet account of Barisal Deputy Commissioner Office in 2003. The incident was revealed after the Deputy Commissioner Office received a heavily bloated Internet bill whereby a complaint was lodged with the Bangladesh Tar and Telephone Board (BTTB).[20]

vi. 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."[21]

vii. Hacking the mail of BRAC[22] Bangladesh.

viii. Stealing the transaction report of Dhaka Stock Exchange through hacking.[23]

ix. Inserting naked pictures to the website of Bangladesh National Assembly.[24]

x. Inserting naked pictures into the website of Jamate Islami Bangladesh.[25]

xi. Inserting naked pictures into the website of the Daily Jugantor.[26]

xii. E-mail threatening to the Dhaka Office of the World Bank.[27]

---

8. Bangladesh Computer Society Website Hacked By Libyan Hacker, Reported by Staff Reporter Shimul, DNews, available at http : // www. cnewsvoice .com (accessed 3March2015).
19The Daily Star Web Edition, vol.5, no.94, 2004. Available at http// www.thedaily.net/2004/08/27/d4082701055.htm.(accessed 3 July 2015).
20. The Daily Star, Sunday, July 13, 2003.
21. http ://www.thedailystar.net/archive.php?date=2008-09-06.
22. BRAC, an international development organization based in Bangladesh, is the largest non-governmental development organization in the world.
23. Ibid
24. Ibid
25. Ibid
26. Ibid
27. Ibid

6. Cyber Crimes Characterised

Founding fathers of internet hardly had any idea, at the time when internet was developed, that internet could also be misused for criminal activities. Presently it is a real fact that it is happening roughly and largely all over the world. Now the question is how these offences could be treated by conventional or extraordinary methods. It is proved that apparently there is no great difference between conventional crimes and cyber crimes. The first demarcating line between the two is the medium of committing a particular crime. Conventional crimes are *prima facie* territorial and occurred in physical world, but cyber crimes are not limited to territorial boundaries as they occur in the world which is an electronic or virtual one. A major question may arise regarding the nature of the cyber crimes that whether they are criminal offences or civil wrongs or a tort. The answer would depend on the nature of the incident. Under the Information and Communication Technology Act, 2006 all the aforesaid computer-based crimes are treated as criminal offences.

7. Remedies Available and their Lacking

'Prevention is better than cure' is a wise saying. For the prevention of numerous cyber crimes it is better to initiate advanced technological actions or technological precautionary measures. But as the time runs along with computer-civilization, an attempt may be taken to cure the alleged cyber crimes, for which legal and other remedies and their lacking available in Bangladesh are to be found out. A cyber victim in Bangladesh has a better opportunity to get proper remedy under the ICT Act, 2006. The statute is the first of the kind in Bangladesh and the only door open for lawful remedy against various cyber crimes in the country. Through this statute it is being tried to locate all the 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 internet, changing source code, stealing or damaging any text, audio, video

documents etc. Provisions for special Cyber Tribunals[28] having both original and appellate jurisdictions and punishments of lighter or severe form have been fixed. Mass people are not much aware about such types of crimes and the procedure of remedies against them. Under the provisions of the ICT Act a number of other procedural and structural hurdles are found to exist which are as follows :

Firstly; Under the ICT Act of 2006 a Sessions Judge or an Additional Session Judge is to preside over the Cyber Tribunal.[29] A Tribunal[30] which includes a Chairman, who may be an ex or acting judge or a competent person to be a judge of the Supreme Court, and two members one of whom should be an ex or acting District Judge and the other an ICT expert. Like other criminal cases Public Prosecutors are to prosecute on behalf of the State. The problem that may arise here is that judges and the lawyers are the experts of laws, not of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the oppórtunity to be assisted by the ICT expert. But is it possible to give verdict on the basis of another's knowledge? The reality in our country is that so long as no initiative is taken by the Government to train up the judges of the Tribunals for acquiring proper technological knowledge no justice can, in this respect, be ensured.

Secondly; A police officer not below the rank of a Sub-Inspector can be an Investigation Officer (IO)[31] regarding cyber crimes. Like the judges, police officers also under the law may have no opportunity to gather required technological knowledge due to lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. Is it, then, possible for such a police officer to make proper investigation

---

28. The Information and Communication Technology Act, 2006, Sec : 68, 82.
29. Ibid, Sec 68(2)
30. Ibid Sec 82(2)(3)
31. Ibid Sec 69(1)

into the matters in dispute? 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 formulating terms and conditions of the service of the Judges of the proposed tribunals.[32] 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 rule of law. But present 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 the aforementioned problems demands that the State must take nippy steps along with logistic and financial assistance.

8. Some New Dimensions as Remedies against Cyber Crimes

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 advanced in technology can smash the security wall anytime. So, legal and other related remedies are a must for fighting the war against the said evils. 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.[33] Constitution plays the mother role in preserving and ensuring the rights and duties of both the State and the 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 technologies

---

32. Ibid, Sec 82(4)
33. Art.7, Constitution of the People's Republic of Bangladesh.

to ensure peaceful cyber cloud. Cyber criminals are not the rivals of any specific country or of a region; 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 merely. The Police Force through global partnership need to be able to meet the challenges of the technology to curb all crimes including cyber crimes. U.K., U.S.A, India, Malaysia and some other developed countries have established special wings of police to combat 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 23rd July 2009 North Korea twisted 'Korea Internet and Security agency'[34], a government agency uniting three of its preceding internet technology organizations. The agency endeavours to make North Korea a stronger, safe and more 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 crimes in Bangladesh, the Government may commence such types of agencies. The worth of such agencies is that these may be able to perform multidimensional actions like advancing internet infrastructure, maintaining the ISPs[35], fixing internet using charges, preventing cyber threats etc.

iv. Watch Dog Groups : A person or group of intelligence persons that acts as a protector or guardian against internet inefficiency, illegal practices, etc. They include capturing and receiving malicious software, disassembling, sandboxing, and analyzing viruses and trojans, monitoring and reporting on malicious

---

34. Korea Internet and Security Agency, available at http :// www.nida.or.kr/kisa/eng/english_ver.html,(accessed 1 May 2015).
35. An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

attackers, disseminating cyber threat information etc. This doggy concept is not a new one. 'Shadow Server Foundation' can be an example of Watch Dog Group which was established in 2004. These may be private 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 mainly common people become the victims of cyber threats and millions of computers are crashed away. If it be possible to make populace aware about the nature of cyber crimes, possible impairment and antidote of the threats, it may be more convenient to defeat cyber criminals that may save the virtual world. Like other vital issues, the Government, therefore, should create awareness among mass people all over the country through different media. Besides, NGOs[36] and other organizations can commence campaign in this regard.

9. Terms and Concepts as Accommodated in the Book

The title of this book may require thinking of the following terms and concepts.

i. **Internet :** The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer. Section 2(8) of the ICT ACT, 2006[37] provides that "Internet" means such an international computer network by which users of computer, cellular phone or any other electronic system around the globe can

---

36. A non-governmental organization (NGO) is an organization that is neither a part of a government nor a conventional for-profit business. Usually set up by ordinary citizens, NGOs may be funded by governments, foundations, businesses, or private persons.
37. Act no 39 0f 2006.

communicate with one another and interchange information and can browse the information presented in the websites.

ii. **Worldwide Web :** The Web, or World Wide Web, is Basicallya system of Internetservers that support specially formatted documents. The documents are formatted in a markup language called HTML (*HyperText Markup Language*) that supports links to other documents, as well as graphics, audio, and video files.
This means it can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

iii. **HTML :** HTML (Hypertext Markup Language) is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. Each individual markup code is referred to as an element, some elements come in pairs that indicate when some display effect is to begin and when it is to end.[38]

iv. **Cyber Property :** In cyberspace, property is not a commodity, but a place. It is distinct from the meaning of traditional property.

v. **Cyber Jurisprudence** : Cyber Jurisprudence like any other jural science is the study of laws relating to cyber. While technology conquers the physical world at an unimaginable speed, the issues concerning its regulatory aspects are also on the looming, posing concerns for jurists all over the world. Since the world "cyber" knows no National boundary, any such regulations require to have international outlook and uniformity, necessitating collective and several efforts of nations across the globe. Cyber technology is a double edged weapon - a menace in

38. Z. Ahmed, op. cit., p.6.

wrong hands and unless regulated it is more dangerous than nuclear weapon. Therefore, even though a nascent entrant in the sphere of law, cyber jurisprudence poses national as well as international nuances.

vi. **Digital Signature :** "digital signature" [39]means data in an electronic form, which– (a) is related with any other electronic data directly or logically; and (b) is able to satisfy the following conditions for validating the digital signature– (i) affixing with the signatory uniquely; (ii) capable to identify the signatory; (iii) created in safe manner or using a means under the sole control of the signatory; and (iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

vii. **Electronic Form :** "electronic form"[40] with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device or technology.

viii. **Electronic Record :** "electronic record"[41] means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

ix. **Electronic Mail :** electronic mail[42]" means information generated electronically and transmitted using internet.

x. **Data :** "data"[43] means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has

---

39. Section 2(1) ICT Act of 2006(Act no 39 of 2006)
40. S.2(5),Ibid.
41. S.2(7)Ibid.
42. S.2(9)Ibid.
43. S.2(10)Ibid.

been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer.

xi. **Computer :** "computer"[44] means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

xii. **Subscriber :** "subscriber"[45] means a person in whose name the Digital Signature Certificate is issued.

xiv. **Civil Procedure :** "Civil Procedure"[46] means Code of Civil Procedure, 1908 (Act V of 1908).

xv. **Penal Code :** "penal code"[47] means Penal Code, 1860 (Act XLV of 1860).

xvi. **Cyber Tribunal :** "cyber tribunal"[48] or "tribunal" means a cyber tribunal constituted under section 68 of ICT Act, 2006.

xvii. **Cyber Appeal Tribunal :** "cyber appeal tribunal"[49] means a cyber appeal tribunal constituted under section 82 of ICT Act, 2006.

---

44. S.2(13)Ibid.
45. S.2(15)Ibid.
46. S.2(17)Ibid.
47. S.2(18)Ibid.
48. S.2(38)Ibid.
49. S.2(38)Ibid.

10. Conclusion

Bangladesh is trying best to be a middle-economic country. 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 a great lacking. The State should move forward to create such experts with indispensable national ventures. Statutory shields should be made most effective by executing the aforesaid course of actions. Finally, it is to be remembered that technology is changing nature and direction every moment that needs maximum capability on part of the people to fight against both in physical and virtual world for a perpetual existence of a gentle global and municipal civilization.

CHAPTER-TWO
Cyber Jurisprudence and Jurisdiction of Cyber Law

1. Cyber Jurisprudence

1. Cyber Jurisprudence

Cyber jurisprudence is a legal term that refers to the concepts that govern cyberspace[1] and the internet.[2] The growth of fresh dimensions in law has been aided by the emergence of cyber jurisprudence around the world. Students and professionals who are interested in learning more about this unique and young subject of study have opened doors to new opportunities all across the world.

Similar issues will arise in the future in a variety of virtual space transactions, and we should psychologically prepare ourselves to adopt new conceptions of virtual property and laws governing virtual property. Of course, the first step is to apply existing physical society notions to virtual space, but we will eventually need to develop separate Cyber Jurisprudence to deal with such issues. For example, if the Bragg case[3] is determined in Bangladesh, the transfer should be governed by the "Transfer of Property Act" and the "Registration Act," as the nature of the property is "Land." The Transfer of Property Act, on the other hand, does not recognize "virtual land" as an immovable property, hence the transaction would be invalid under its terms.

---

1. Cyberspace is interconnected technology. The term entered the popular culture from science fiction and the arts but is now used by technology strategists, security professionals, government, military and industry leaders and entrepreneurs to describe the domain of the global technology environment.
2. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
3. Bragg v. Linden Research, Inc. - 487 F. Supp. 2d 593 (E.D. Pa. 2007).

Because the way the virtual property is used is a "Creation in the thoughts of an imaginative participant," certain of its attributes give it a "Intellectual Property Character." As a result, the disagreement should not be classified as a "Transfer of Property Dispute" or a "Contractual Property Dispute." Even if IPR rules such as copyright are the most closely related to the property, they do not pass the "Meeting of Minds" criteria.

It is observed that in recent judicial reviews, whenever implementation of existing laws of the real space to Cyber Space has encountered a conflict, the laws of the real space has prevailed. This tendency in due course is likely to develop into a principle of "Primacy of Meta Space" and become the bedrock of Jurisprudence.[4] However, when two laws of the real space itself come to conflict in the Cyber Space, the principle of "Primacy of the Meta Space" fails. This is reflected mainly in IPR[5] disputes and Jurisdiction disputes. Instead of fighting legal battles that can only end in victories for the one who has more financial resources, it is necessary to accept that "Real World Laws Cannot be Extended for Every Conflict in Cyber Space"

Now is the time, not when a Crisis occurs, when we should examine cyber jurisprudence in a cyber-society.[6] Left to their own devices, lawyers have a way of siphoning the joy out of anything. Stories like Bragg's probably have most attorneys drafting retainers for the personal injury claims of the 21st century rather than trying to shape a sustainable legal framework for cyber society. As we have discovered in the real world, the Internet has rarely offered easy opportunities to co-opt existing law. Yet, we are presented with an unprecedented opportunity to re-imagine the role of law, to redefine

---

4. Ahmed, Dr. Zulfiquar; Cyber Law in Bangladesh, Published by- Sheikh Mohammad Ali Hasan, National Law Book Company, Nilkhet, Dhaka-1205. P. 36-37
5. Intellectual Property Right.
6. Human-computer interaction has progressed to the point where the term "cyber society" has been coined. This relationship (human-computer interaction) comprises the relationship between a society of humans and a network of computers, not just a single human and a single computer.

its relation with people, to create a legal system heretofore undreamed of. The architects of Second Life, Wikipedia, and others are anything but traditional.[7]

Cyber jurisprudence gives an analysis of the law where, is no land and even there is no border, where all things may be different from the physical world, they may be virtual from origin and nature. We may find virtual world with virtual rules and policies, along with the virtual subject matter, virtual contract, virtual disputes, virtual property, virtual possession and virtual court. Cyber jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace. It emphasis to recognize cyber uniform rules and policies at international level.[8]

Legal issues relating to the electronic and internet in this contemporary world as being necessitated of new kind of jurisprudence, which may be cyber jurisprudence. Cyber jurisprudence gives an analysis of the law where, is no land and even there is no border, where all things may be different from the physical world, they may be virtual from origin and nature.

Cyber jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace. It emphasis to recognize cyber uniform rules and policies at international level, it also discusses with the netizens[9] and netiquates.[10]

2. Claiming new dynamism in jurisprudence

During the preceding decade, the Internet has grown dramatically. Over 9.4 million computers and up to 40 million people are now connected to the Internet, according to estimates. By the end of the century, there will almost certainly be over 200 million Internet users. Without a doubt, cyber law is a promising topic.

---

7. Ibid. P. 38-39
8. http://www.bloggernews.net/11215
9. The term netizen is a portmanteau of the words Internet and citizen as in "citizen of the net". It describes a person actively involved in online communities or the Internet in general.
10. Netiquette is short for "Internet etiquette." Just like etiquette is a code of polite behavior in society, netiquette is a code of good behavior on the Internet.

Cyber law covers cybercrime, online trade, freedom of expression, intellectual property rights, and privacy rights. Cybercrime includes credit card fraud, unlawful access to computer systems, child pornography, software piracy, and cyber stalking. It's worth emphasizing that in order to identify cybercrime and cyber criminals, as well as to resolve jurisdictional confusion, cyberspace architecture and access channels must be addressed.

3. Genesis & the architectural factors of cyber territory

The Internet mechanism can be considered as the global connection of interconnected computer networks straddling state and national borders. The perception of interconnecting computers originally commenced in 1969 as part of a military program called "ARPANET."

4. Territorial monopoly versus cyber space

The law is conceived and spoken of as territorial .the enforcement of law is undoubtedly territorial in the same way as the state is territorial; that is to say the state power is in time of peace exercised only within the territory of the state on its public ships and aircraft and on vessels and aircraft registered under its law.

But the law applicable to the cyber space is quite different form territorial –based law because of the peculiarity of cyber world bearing virtual character of visual nature. It should be considered that the events or activities ensued in cyber world causing legal consequences are not less than those in the real world are.

Accordingly a distinct set of laws and legal principles has become inevitable to be adopted with same mission holding sprit of punishment or remedy. The financial damage sustained by the individual or by corporate body or by governmental organs is claiming billions of dollars, which sometimes surpass traditional territorial-based damage.

5. Jurisdictional confusion

The developing law on jurisdiction must address whether a specific event in Cyberspace is governed by the laws of the state or

country in which the Website is located, the laws of the state or country in which the Internet service provider is located, the laws of the state or country in which the user is located, or perhaps all of these laws.

A number of observers have suggested that cyberspace be considered as a distinct jurisdiction. In practice, the courts haven't agreed with this viewpoint, and legislatures in many states[11] haven't addressed it.

Courts must balance numerous issues when deciding lawsuits involving foreign nationals. Courts must evaluate the procedural and substantive policies of foreign countries whose interests are impacted by the court's assertion of jurisdiction on a case-by-case basis. When extending authority into the international realm, extreme caution and caution are required. When suing a foreign national, there is a greater jurisdictional bar because of the principle of sovereign equality.

6. Cyber terrorism, a real menace

It fear is measureless, its impact is great, its target is human race, it exist somewhere around us, but invisible. It may occur anytime anywhere in the world. It has not been experienced even imagined by man of today, in past. It may reshape in any form. Its alarming aspect is to be developed as an ideology. Its intensity of destruction may severe more than devastation, man of our age ever be thought. No man or country obviously favor or supports it but surprisingly it is being faced by every man and every country. It is unfortunately new phenomenon, it is terrorism in the real world or it may be cyber terrorism in cyberspace.

To define the cyber terrorism many analysts and internet intellectuals draw the almost same parameters, Mark Pollitte of Federal Bureau of Investigation defines the cyber terrorism as follow;

Cyber Terrorism is, "the premeditated, politically motivated attack against information, computer systems, computer programs,

---

11. http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html

and data which results in violence against noncombatant targets by sub-national groups or clandestine agents".

Computer technology and internet is going to be indispensable part of to-day society and advanced country are becoming more and more dependant and reliant of computer and internet technology. The critics who criticized the John Arquilla who depicted a scenario of mayhem of destruction by cyber terrorism, now are reconsidering their ideas and criticism after the unfortunate terrorist event of 9/11 in USA.[12]

Cyber terrorism can affect a specific community of people as well as entire nation, the example of Australian man in 2001 would be amplify when he used the internet and stolen control software to release one million liters of raw sewage in the public park, but his intention was not to terrorise the people but just to get back it job in the concerned company. A more baleful Cyber Terrorism intrigue that was stymied would have occurred sometime in 1996 in London (2003). Members of the Irish Republican Army were planning to blow up and destroy six key electric substations in London. Had the IRA succeeded in their goal, they would have disrupted power to major portions of London for months. To figure out which substations to bomb, they used libraries and open sources of information to select key nodes that would impact the grid the most. This example would have been a terror attack and would have stuck fear into the people of London. This would also be an example of a physical attack on computer systems.

According to The Guardian, "Nato is treating the threat of cyber warfare as seriously as the risk of a missile strike". If a Governmental Organization like NATO thinks that cyber warfare is that dangerous, then why don't more people think of it that way. The reason for this could be that the general population of the world does not feel the impact of these cyber terrorist attacks.

Cyber terrorism has been accruing with last twenty years and as time progressed and more and more nations become even more computerized, there will be more and more attacks through internet.

---

12. "http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html"

The measures are available to counter the cyber terrorism as US Department Defense charged with the USSD with duty if combating the cyber terrorism. The sensitive data can be safe and secure by the 'air tight' mechanism which has adopted by the FBI successfully. Up to date Antivirus system, firewall and root-kit can play important role to protect the internet and computer system. Intrusion detection system can also help if someone's network has been attacked. A network also requires VPN's if they were people accessing network remotely. In the last but not least exemplary punishments and fine should introduce through the laws against the cyber terrorists as the Pakistan has introduce the Prevention of Electronic Crime Ordinance 2007 where Section 17 exemplary punishments has been provided for the cyber terrorists.[13]

The contemporary world is declared to be a global village, collective efforts of the global nations against this menace to next to this human civilization, can provide potential preventive measures against the cyber-criminal and cyber terrorists. The existence of cyber terrorism cannot be denied it's real but it would be blissful for mankind not to record a single exact cyber terrorist event in its history.

2. Jurisdiction of Cyber Law

1. Establishment and Jurisdiction of Cyber Tribunal in Bangladesh

Government of Bangladesh by gazette notification, for the purpose of quick and effective trial of crimes committed under the Act, may establish one or more cyber tribunal, sometimes which is stated later as tribunal under section 68(1) of the ICT Act. The cyber tribunal that is stated in section (1) of the section will comprise of a session judge or an assistant session judge appointed by the government with consulting with the Supreme Court; and such a judge appointed will be introduced —judge, cyber tribunal.[14]

---

13. "http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html"
14. The information and Communication Technology Act, 2006, S. 68(2)

The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act.[15]

The special tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order.[16]

2. Establishment & Jurisdiction of Cyber Appellate Tribunal in Bangladesh

The ICT Act envisages the establishment of the Cyber Appellate Tribunal at one or more places as the government may deem fit. Section 82(1) of the ICT Act provides that the government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The cyber appellate tribunal will be comprised of a chairman and two members appointed by the government.[17]

The chairman will be such a person, who was a justice of the Supreme Court or is continuing his post or capable to be appointed as such and one of the member will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed.[18]

The chairman and the members will be in their post minimum 3 years and maximum 5 years and the conditions of their service will be decided by the governments.[19]

The Cyber Appellate Tribunal shall have the power to hear and settle the appeal made against the judgment of cyber tribunal and session courts.[20]

The appeal tribunal will have authority of supporting, canceling, changing, or editing the judgment of the cyber tribunal.[21]

---

15. Ibid., s. 68(3)
16. Ibid., s. 68(4)
17. Ibid., s. 82(2)
18. Ibid., s. 82(3)
19. Ibid., s. 82(4)
20. Ibid., s. 83(1)
21. Ibid., s. 83(2)

The decision of the appellate tribunal will be final. The Cyber Appellate Tribunal does not seem to be vested with any original jurisdiction; it has been vested with the powers of a Civil Court in respect of, interlay

a) Summoning and examining of witnesses
b) Requiring production of document
c) Receiving evidence
d) Issuing commissions and
e) Reviewing its decisions.[22]

3. Punishment for Cyber Crime in Bangladesh

The following activities are regarded as offence according to section-54, such as; If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,—

a) Accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so[23]
b) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) Damages or causes to be damaged willingly to any computer, computer system or computer network. data, computer database or any other programmers residing in such computer, computer system or computer network;
e) Disrupts or causes disruption of any computer, computer system or computer network;

---

22. Zulfiquar Ahmed, pp. 150-152
23. The information and Communication Technology Act, 2006, S. 54(a)

f) Denies of causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network, in contravention of the provisions of this Act, rules or regulations made there under;

h) for the purpose of advertisement of goods and services, generates or causes generation of spasm or sends unwanted electronic mails without any permission of the originator or subscriber;

i) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network. If any person commits any of the aforesaid offence, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both. The ICT Act describe punishment for tampering with computer source code is if any person intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network. When the computer source code is required to be kept or maintained by any law for time being in force, then this activity of his will be regarded as offence.[24]

Whoever commits this type of offence shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to Taka three lakhs, or with both. The ICT Act describe punishment for hacking with computer system is if any person, intentionally cause wrongful loss or damage to the public or

---

24. Ibid., s. 55

any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.[25]

or cause damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him; then such activity shall be treated as hacking offence.[26]

Whoever commits hacking offence, he shall be punishable with imprisonment for a term which may extend to ten years, or with time which may extend to Taka one crore, or withboth.The ICT Act describe punishment for publishing fake, obscene or defaming information in electronic form is if any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene orits effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.[27]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to ten years and with fine which may extend to Taka one crore. The ICT Act describe punishment for misrepresentation and obscuring information is if any person makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate shall be regarded as an offence[28]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or

---

25. Ibid., s. 56(1)
26. Ibid., s. 56(2)
27. Ibid., s. 57
28. Ibid., s. 62

with fine which may extend to Taka two lakhs, or with both. The ICT Act describe punishment for disclosure of confidentiality and privacy is no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.[29]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or with time which may extend to Taka two lakhs, or with both. The ICT Act describe punishment for using computer for committing an offence is whosoever knowingly assists committing crimes under this Act, using any computer, e-mailor computer network, resource or system shall be regarded as an offence.[30]

Whoever aids committing these types of offence he shall be punishable with the punishment provided for the core offence. The ICT Act describe punishment for Offences committed by companies etc then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.[31]

4. Cases under ICT Law in Bangladesh

Bangladesh does not have enough natural resource and has 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

---

29. Ibid., s. 63
30. Ibid., s. 66
31. Ibid., s. 67

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.[32]

The present government has also declared the vision2021 i.e. within 2021 this country will become Digital Country and the percaptia income will be equal to a middle income country. But the government as well as other concerns should consider crimes that they may be committed in this world with the expansion of internet and her/networks to convert this country.

32 https://www.thedailystar.net/drivers-economy/ict-opens-new-prospects-

CHAPTER THREE

The Right to Freedom of Opinion and Expression under the Cyber Legislation in Bangladesh

1. Introduction

Everyone has the right to express themselves freely. This right of someone may be limited in order to preserve the goodwill and reputation of others. Any restriction on the right to freedom of expression imposed by law is unconstitutional. For the sake of preserving a democratic society, the limitation may be acceptable. In any civil society, the use of one's freedom to freely express one's viewpoint via speech, writing, and other means of communication in a way that intentionally and willingly causes damage to others' character and/or reputation through false or misleading remarks may be deemed unnecessary. The unwarranted use of a right may result in inappropriate and undesirable behavior, which may be punishable under Bangladesh's Penal Code (Act No. V of) 1860 or the Information and Communication Technology Act[1] (No. 39 of) 2006. Even yet, it is possible that it will lead to certain crimes that are not covered by the Act of 2006, since many cyber-crimes or digital crimes, such as crimes committed using mobile phones,[2] are not covered by the Act of 2006.

Different kinds of cyber crimes are seen to develop and continue in the present world including Bangladesh. Hacking or unauthorized entry into information systems, virus introduction, Publishing or distribution of obscene content in electronic form, tampering with

---

1. Act No. 39 of 2006.
2. This law makes e-mails evidence which supplements the country's Evidence Act of 1872. Even the amendments to the ICT Act (Amended in 2013) did not address the issues.

electronic documents required to be kept under law, frauds using electronic documents, Violation of privacy rights such as Stalking, violation of copyright, trademark or patent design, Defamation through e-mail, holdings out threats through e-mail etc. are examples thereof.

2. An Overview of the Cyber Legislations in Bangladesh

2.1. Objectives of the Cyber Legislations

The objectives of the cyber legislation i.e. the ICT Act, 2006 has been provided for the purposes like easing the progress of electronic filing of documents with government agencies and statutory corporations and to promoting efficient delivery of government services by means of reliable electronic records.

Helping establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records, facilitating electronic commerce, eliminating barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and promoting the development of the legal and business infrastructure necessary to secure electronic commerce etc are also included in the objectives.

The work is conducted to identify the provisions of the Information and Communication Technology Act of 2006 violating the right to freedom of expression and limiting the legitimate right of individuals to comment on public matters that goes against the Government, consider the implementation of the ICT Act of 2006 and its impact on the freedom of opinion and expression and cyber crimes. It also examines the existence of mechanisms in the Act that can hold in check the chance of its provisions being abused thereby violating the right to freedom of expression and limiting the legitimate exercise the right to comment on public matters which might contain criticisms against the Government.

2.2. Weaknesses of the Cyber Legislations in Bangladesh

There are several flaws in the Information and Communication Technology Act. The social norm and regulation of information technology are sometimes regulated by the law. As a result, although

the legislation addresses intellectual property rights, it does not address the rights and responsibilities of domain[3] name proprietors, which is the first step in e-commerce.[4] Under section 76 of the ICT Act 2006, the crimes are not cognizable (2). To get redress, the victim must submit a complaint with the appropriate law enforcement authorities. This is the Act's most serious flaw. In section 68 of the Act, it was stated that a special tribunal known as the Cyber Tribunal would be created in each district of Bangladesh. However, in the Dhaka area, just one Tribunal has been formed thus far.

Because of the dependency of the laymen on the technology specialists and well trained lawyers and judges the disposal of cyber cases are rare. The few number of cases which are filed are found to be pending. To remove such kind of pendency of cases the judges, lawyer and specialists should be well trained and skilled.

The Bangladesh police has a special branch named "Anti-Cyber Crime Department" headed by a Deputy Commissioner of Police to protect e-mail fraud, threat by e-mail, defamation or publication of unauthorized pictures. The Department is yet to fulfil the public demand due to the scarcity of well trained man power. A case cannot start due to the non visibility of the plaintiff. There is no scope for the state to take liabilities as being a plaintiff.

The Cyber Tribunal has not yet inflicted any punishment to any criminal. Due to this the criminals are continuing to commit crimes

---

3. There are several flaws in the Information and Communication Technology Act. The social norm and regulation of information technology are sometimes regulated by the law. As a result, although the legislation addresses intellectual property rights, it does not address the rights and responsibilities of domain name proprietors, which is the first step in e-commerce. Under section 76 of the ICT Act 2006, the crimes are not cognizable (2). To get redress, the victim must submit a complaint with the appropriate law enforcement authorities. This is the Act's most serious flaw. In section 68 of the Act, it was stated that a special tribunal known as the Cyber Tribunal would be created in each district of Bangladesh. However, in the Dhaka area, just one Tribunal has been formed thus far.
4. Electronic commerce, commonly known as e-commerce or ecommerce, is trading in products or services using computer networks.

thinking that they would not be punished. This is one of the main weaknesses of the implementation of the Bangladesh Information & Communication Technology Act of 2006.

2.3. Advantages of Cyber Legislations

The 2006 Information and Communication Technology Act includes several drawbacks as well as benefits. The law establishes a legal definition for the notion of "safe digital signatures," which must pass through a government-mandated security process. Companies, on the other hand, may engage in internet trade.

Using the legal infrastructure that the law provides. As a result of this law, additional facilities for running a cyber or information and technology company were available.

However, as the country's use of the internet has increased, there has been a growing need to establish suitable cyber laws, which are necessary for legalizing and regulating the internet in Bangladesh. Even with the most liberal and moderate interpretation, Bangladesh's current laws could not be construed in light of the promising internet. It is anticipated that the relevant authorities would take measures to improve the country's current cyber legislation.

3. Meaning of Freedom of Speech and Expression

Concepts of freedom of speech can be found in early human rights documents.[5] England's Bill of Rights of 1689 granted 'freedom of speech in Parliament' and is still in effect. The Declaration of the Rights of Man and of the Citizen, adopted during the French Revolution in 1789, specifically affirmed freedom of speech as an inalienable right.[6] The Declaration provides for freedom of expression in Article 11, which states that *the free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as*

---

5. Smith, David (2006-02-05); "Timeline : a history of free speech"; *The Guardian*, London, Retrieved 2nd May,2010.
6. Ibid.

shall be defined by law.[7] Article 19 of the Universal Declaration of Human Rights, adopted in 1948, states that *everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*[8]

Today freedom of speech or the freedom of expression is recognized in international and regional human rights laws. The right is enshrined in Article 19 of the International Covenant on Civil and Political Rights of 1966, Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950,

Article 13 of the American Convention on Human Rights of 1969 and Article 9 of the African Charter on Human and Peoples' Rights of 1981. Based on John Milton's arguments, freedom of speech is understood as a multi-faceted right that includes not only the right to express or disseminate information and ideas, but three further distinct aspects : (a) the right to seek information and ideas, (b) the right to receive information and ideas, and (c) the right to impart information and ideas.

International, regional and national standards also recognize that freedom of speech, as the freedom of expression, includes any medium, be it oral, written or in print, through the internet or through art forms. This means that the protection of freedom of speech as a right includes not only the content but also the means of expression. In the key case *Handyside v. UK(1976)*[9] the European Court of Human Rights declared that freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for the development of everyman....it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but

---

7. "Declaration of the Rights of Man and of the Citizen", available at www.hrcr.org, (accessed 3 February 2014). On this point may be seen A.W. Diamond, Law Library at Columbia Law School, 2008.
8. "The Universal Declaration of Human Rights", available at www.un.org. (accessed 3 February 2014).
9. 1EHRR 737.

also to those that offend, shock or disturb...such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'.

4. Critical Analysis of the ICT Act of 2006 of Bangladesh

The Information and Communication Technology Act of 2006 of Bangladesh provides for the legal infrastructure for e-commerce. The Act enables (a) legal recognition of electronic transaction, (b) legal recognition of digital signature, (c) acceptance to contract 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, forgery or falsification in e-commerce and electronic transaction, and (h) other solutions.

The objectives of the ICT Act of 2006 are to facilitate the progress in electronic filing of documents with government agencies and statutory corporations, to promote efficient delivery of government services by means of reliable electronic records and to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements. The law may be a law for digital signature and authentication of e-communication not to regulate the internet activities and crimes.

The Government of Bangladesh used sections 46 and 57 of the ICT Act to ban the social networking site Facebook in May 2010. After the ban was imposed sections 46 and 57 of the ICT Act were challenged in the High Court Division of the Supreme of Bangladesh by Barrister Arafat Husen Khan, Kazi Ataul-Al-Osman, and Rokeya Chowdhury.[10] The High Court Division asked the Government to show cause why the sections of the ICT Act should not be held unconstitutional for violating the right to freedom of expression.

Instead of amending the ICT Act to ensure compliance with the Bangladesh Constitution and Bangladesh's international law

---

10. *Arafat Hosen Khan and others v. Bangladesh and others*,2010, Writ Petition No 4719, HCD, SC, BD.

obligations the Government revised the ICT Act through an Ordinance of 20 August 2013 in a way that makes it less in line with human rights norms. On 6 October 2013 the Bangladeshi Parliament passed the Information and Communication Technology (Amendment) Act 2013 incorporating the provisions of the Ordinance into the ICT Act.[11] The amendments made many offences under the Act non-bailable[12] and cognizable.[13] The amendments also imposed a minimum sentence of seven years of imprisonment for offences under the Act and increased the maximum penalty for offences under the law from ten to fourteen years' imprisonment.

The objective of the ICT Act, as stated, is the legal recognition and security of information and communication technology. The amendments to the Act appear to be designed to stifle the legitimate exercise of public criticism and to subject various persons including journalists, bloggers and human rights defenders to arbitrary detention.

The original ICT Act of 2006 contains a number of vague, imprecise and overbroad provisions that serve to criminalize the use of computers for a wide range of activities in contravention of the right to freedom of expression including the right to receive and impart information protected under international law. Although the right to freedom of information is not absolute the restrictions contemplated under the Act do not fall within the scope of exceptions permissible under international law including Bangladesh's treaty obligations. Section 46 of the original ICT Act, for example, grants powers to the Government to direct any law-enforcing agency to restrict information through any computer

---

11. Articles 80(1), (2) & (5) of the Constitution of Bangladesh of 1972 provide that every proposal in the Parliament for making law shall be made in the form of a Bill. When a Bill is passed by the Parliament it shall be presented to the President for assent. When the President has assented or is deemed to have assented to a Bill passed by the Parliament it shall become law and shall be called an Act of Parliament.
12. In non-bailable offences bail is not granted as a matter of right. The accused is required to apply to the court, and granting bail is at the discretion of the court.
13. If an offence is cognizable the police may arrest persons suspected of committing the offence without an arrest warrant.

resource if, in their opinion, such prevention is...*necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to commission of any cognizable offence.* Section 57 of the original ICT Act criminalized publishing or transmitting or causing to publish or transmit ...*any material which is fake and obscene or its effect is such as to tend to corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.*

The ICT (Amendment) Act of 2013 makes the law less in compliance with Bangladesh's human rights obligations. Under the original Act the police had to take permission from the Home Ministry before registering a case under the law. The amended Act makes offences under sections 54, 56, 57 and 61 cognizable, allowing the police to make arrests without a judicial warrant. In addition, under the amended Act, offences prescribed by sections 54, 56, 57 and 61 are made non-bailable. The amended Act also increases the maximum sentence for offences under sections 54, 56 and 57 of the Act from 10 to 14 years of imprisonment and prescribed a minimum sentence of seven years. The amended law retains the optional fine of ten million taka. Unfortunately some of the features of the Act may be considered a barrier to the freedom of expression. For instance, according to Article 57 of ICT Act 2006 (Amended in 2013) any wilful release on websites or any other electronic platform of any material which is false, vulgar, defamatory, liable to cause deterioration of law and order, or tarnishes the image of the state or individual, or hurts religious sentiments is treated as a cyber crime.

There are some loopholes in the Act. They are as follows :

(i) If a person uploads his/her opinion in Facebook providing some information on some political issues and if the

information be wrong its source being a wrong report of a newspaper he/she may become a victim since the Government is able to file a case against him/her. Again, in section 57 of the ICT Act 2006 (Amended in 2013) the word 'vulgar' is an ambiguous one. How is it to define the term 'vulgar'? So, it can be argued that this Act is also a threat to freedom of expression.

(ii) In the network environment creation of fake identity, for instance e-mail address, Facebook identity etc., in any other person's name is quite easy in the cyberspace. So a criminal may, by uploading offensive materials using some other person's name, intentionally victimise that person. In law there is no indication of how to resolve such a sort of problem. The new amendment of the ICT Act considers cyber crime a non-bailable one. There is no guarantee that this Act will not be used as a political weapon just to harass political opponents. As known earlier, cyber crime may be global in nature. The Act does not address the point.

(iii) When enacting any law involving high-tech and complexities the capability of law enforcing agencies must be considered. For this, a special capability building programme must be initiated for the relevant wing of the law enforcing agencies so that they become technologically knowledgeable enough for dealing with this sort of crime.

The ICT Act identifies some critical situation which is not clear to the archaic legal provisions of the country. The law does sometime regulate the social norm and then control information technology. Since the passing of the Information and Communication Technology Act in the Parliament a lot has been said both for and against it.[14] The following points may be addressed here : (i) There are sufficient safeguards in the ICT Act itself which provide that the provisions of the Code of Criminal Procedure, if

14. Z. Ahmed, op.cit., pp. 61-62.

required for the trial of the cyber offence,[15] may apply. (ii) The right to privacy is essential to enable individuals to express themselves freely. The ICT Act and amended provisions, however, don't recognize the right to privacy. As the country does not have any data protection law anyone can be the victim of misuse of the law due to the emergence of the information highway and technological advancements.[16] The Information and Communication Technology (Amendment) Act 2013, therefore, poses a severe threat to the enjoyment of the right to privacy, freedom expression and other human rights in the country.[17]

5. Freedom of Opinion and Expression Issues under the ICT Act of 2006

Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[18] guarantees the right to freedom of opinion and expression, including the right to receive and impart information and ideas of all kinds, regardless of frontiers. It includes political discourse, commentary on one's own and public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse.[19] The Human Rights Committee, the treaty-monitoring body of the ICCPR, affirmed that these rights constitute the foundation-stone for every free and democratic society[20] as they promote accountability, transparency, and the promotion and protection of other human rights. Under

---

15. K. Hossain, *A Compilation of Media and Technology Laws*, Shams Publications, Dhaka, 2011, p. 101.
16. http ://www.voicebd.org/node/417,(accessed 5March 2014).
17. Ibid.
18. International Covenant on Civil and Political Rights of 1966, adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49. The International Covenant on Civil and Political Rights may be called ICCPR throughout the study.
19. UN Human Rights Committee, General Comment 34 UN Doc.no,CCPR/C/GS/34 http ://www2.ohchr.org/english/bodies/hrc/docs/gc34 pdf,para 11.
20. Ibid., para 2.

international law the right to freedom of expression applies to all forms of communication including the internet.[21] Article 19(3) of the ICCPR stipulates specific conditions for any restriction on freedom of opinion and expression. It is found that section 57 of the ICT Act contravenes Bangladesh's obligations under Article 19 of the ICCPR : the offences prescribed are vague and overbroad; the restrictions imposed on freedom of opinion and expression go beyond what is permissible under Article 19(3) of the ICCPR and the restrictions are not necessary and proportional to achieve a legitimate purpose.

Under international law and the general principle of legality criminal offences must be prescribed by law. It means that they must be formulated clearly and precisely so that individuals can regulate their conduct accordingly. States must refrain from restricting freedom of expression through vague, imprecise, and overly broad regulatory language. The Human Rights Committee emphasizes that laws must not confer unfettered discretion for the restriction of freedom of expression to those responsible for their execution and must provide sufficient guidance to enable law enforcers and the general people to determine what kind of expressions are restricted.

It is pertinent to mention that section 76 of the amended ICT Act, which makes some offences under the Act non-bailable, violates the right to liberty and may also undermine the presumption of innocence which must be accorded to the accused under international law.[22] Article 9 of the ICCPR protects the right to liberty and security of the person and provides that it shall not be the general rule that persons awaiting trial shall be detained in custody. Under international law and standards states may only detain individuals pending trial where it is absolutely necessary to ensure his or her presence at trial or preservation of evidence.

The ICCPR provides under Article 9(3) the limited circumstances under which pre-trial detention is permissible. According to the Human Rights Committee, Article 9(3) requires that *pre-trial detention should be the exception and...bail should be*

---

21 . Ibid., para 12.

22. Article 14(2) of the ICCPR

granted, except in situations where the likelihood exists that the accused would abscond or destroy evidence, influence witnesses or flee the jurisdiction of the state party.[23] Provisions of the ICT (Amendment) Act 2013 that make offences under sections 54, 56, 57 and 61 non-bailable are incompatible with Article 9(3) of the ICCPR.

The International Court of Justice is also concerned that long periods of pre-trial detention put accused persons at a risk of torture and other forms of ill-treatment. Human rights groups have documented that torture and other ill-treatment by police is widespread in Bangladesh, especially when they undergo police remand.[24]

6. The Amended ICT Act and Present Situation of Freedom of Opinion and Expression Issues in Bangladesh

The ICT (Amendment) Act, 2013 is a threat to freedom of expression, because it is contradictory both with the Constitution of Bangladesh and Right to Information Act[25] as well as challenges for privacy and Human Rights. The amendment of the ICT law is more about violating citizens' constitutional right to freedom of speech than protecting their liberty.[26] The amended law is pretty inefficient. Technical experts argue that the Government would not be able to

---

23. Communication No. 526/1993, *M. and B. Hill v. Spain*, (views adopted on 2nd April 1997) available at UN doc. *GAOR*, A/52/40, vol. II, p. 17.
24. State of Human Rights 2012, Odhikar, *Chapter V : Torture and other cruel, inhuman or degrading punishment*, January 2013, accessed at : http ://odhikar.org/wp-content/uploads/2013/01/report-Annual-Human-Rights-Report-2012-eng.pdf and Amnesty International, Annual Report 2013, *Bangladesh*, accessed at : http ://www.amnesty.org/en/region/bangladesh/report-2013, section- 13-4
25. The Right to Information Act, 2009 (Act no XX of 2009) has recognised the freedom of expression as an important fundamental right of the citizens and it has made easy dissemination of information from any governmental and non-governmental institutions. But in the ICT Act, there is no clarity as regards 'publication of information' and the type of information that may corrupt others.
26. http ://www.newstoday.com.bd/index.php?option=details&news_id=2363238 &date=2013-12-03, (accessed 7May2015).

tackle cyber-crimes with this kind of inefficient law. The new amendment of ICT Act, for instance, does not cover a majority of crimes committed through mobiles. It considered emails as evidence, which conflicts with the country's law of evidence.[27] The law should thus have included provisions which empower the Government to tackle the growing number of cyber-crimes. But in order to do that the Government should have consulted with all the stakeholders and should come clean by drafting such rules so that they do not prejudice fundamental rights like freedom of speech and expression.

The law under discussion has too many loops to violating right to privacy and as well right to information or freedom of expression. When a citizen expresses something on any social medium which the Government considers offensive or suspicious law enforcers can arrest him or her without prior notice or issuing a warrant. But no individual aggrieved person or victim is allowed to go to the court according to the amended law. Only the law enforcers or the ministry officials are so allowed. An individual, however, may go to law enforcement agencies for their protection. In the near future tribunals may be set up for trying such offenders.

The information and communication technology has a bigger impact in the society, enabling communities to connect to the information highway and allowing for the construction of a digital Bangladesh. However, the amendment in the law has the possibility to enable the abuse of opinions and voices of the citizens and political groups, endangering citizens' right to privacy and human rights at large. It also neglects personal data and privacy protections and people's aspirations for the freedom and democratic practices along with accountability and governance.

---

27. Section 17, 32(Para-2),34,35,39,59,61,62,65,67,68,70 and section 131 of the Evidence Act of 1872 only cover the paper documentation not applicable for electronic based documents. For instance, writing, words printed, lithographed or photographed and a map or plan and an inscription on a metal plate or stone and a caricature are treated documents.

The biggest privacy problem for citizens comes from a disturbing and growing trend of data breaches. This threat to privacy is also a threat to security. In the digital age people are only as safe as computers. But that doesn't mean that they have to adopt an oppressive law. As people are quite concerned about privacy they also are really worried about security and safety. People don't want oppression in the name of protection.

7. Recommendations

In the light of the analysis above the Parliament of Bangladesh can repeal the amendment to the Information and Communication Technology Act (2006) made in 2013 or can modify the ICT Act to bring it in line with international law and standards taking into consideration Bangladesh's legal obligations under the ICCPR. At a minimum the following measures can be adopted for the sake of making the Act more freedom and expression friendly. The followings are, therefore, to be addressed :

i. Amendment of section 57 of the ICT Act so as to ease any contemplated restrictions on freedom of opinion and expression thereby making it consistent with the international law and standards.[28]

ii. Amendment of section 57 of the ICT Act needs to define the prohibited categories of expressions clearly so that its abuse can be minimized or any motivated exploitation of this section can be discouraged.

iii. Amendment of the ICT Act to ensure that any restriction to freedom of expression and information made, including any sanction provided, must be for the sake of a legitimate objective and proportionate to the harm caused by the expressions made.

---

28. e.g. Article 19 of the International Covenant on Civil and Political Rights of 1966, adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49. The International Covenant on Civil and Political Rights may be called ICCPR throughout the study.

iv. Scope of steps should be there to ensure that provisions of the ICT Act are not used to violate the right to freedom of expression, limiting the legitimate exercise of comment on public matters which might contain due criticism against the Government.

v. Scope of dropping charges against bloggers for the legitimate exercise of their freedom of expression.

vi. Direct government agencies should cease to make any politically motivated lawsuits causing unlawful restriction to the exercise of expression and providing compensations to the victims under this provision whose involvements will be found disproportionate to the gravity of the alleged offence.

8. Conclusion

The ICT (Amendment) Act of 2013 sharply conflicts with Articles 39 and 43 of the Constitution of Bangladesh that guarantee right to freedom of expression and right to privacy respectively. The ICT (Amendment) Act of 2013 obviously hampers the right to privacy and data protection, freedom of expression and communication. If it be really necessary to collect someone's personal information by the government authorities or companies they must provide appropriate reason and explanation to this. The demands also include that in a special and emergency situation personal information could be collected with the permission of the owner of the data. It is true that cyber-crimes are on the rise and people have to deal with that within a legal framework. So the Government must adopt new laws as needed. But a law must not defeat its purpose. The amendment of the ICT law is more about violating citizen's constitutional right to freedom of speech than protecting their liberty. Therefore, it is essential for the Government of Bangladesh to substantiate its rationale and necessity for the repressive provisions of the law which is found to be unacceptable in form and substance. The Government is implored to withdraw this amendment to the ICT Act of 2006.

CHAPTER FOUR
Internet Privacy

1. Definition

The degree of privacy and security of personal data disclosed on the Internet is referred to as Internet privacy. It's a broad word that encompasses a wide range of elements, methods, and technologies that are used to safeguard sensitive and private data, communications, and preferences.

Users value privacy and anonymity on the internet, particularly as e-commerce grows in popularity. Theft threats and privacy breaches are typical concerns for every website in development. Online privacy is another term for internet privacy.

The internet is one of the most user-friendly communication technologies ever devised by humanity. It's fast, easy, and inexpensive...and it's just as insecure as it is quick, convenient, and inexpensive. A message written months ago may stay on an ISP's server or as a backup, and anybody who knows how to do so may readily recover it. This is information that you have destroyed for a specific reason : you do not want it to be accessible by others once you have done using it. There have been instances when information was recovered up to 6 months later and utilized as evidence in a court case.

If someone wants to, intercepting your communications or information may be very easy. This might just be an administrator from your ISP or your company's network. It may also be a corporate rival, legal adversary, or government entity with much more severe objectives.

There are a plethora of options for safeguarding your online privacy. Some are big and complicated, while others are quite basic. The key point to remember is that certain techniques are nearly completely insecure, while others are almost impenetrable.

It is a widespread misunderstanding that anonymity equates to privacy. Although anonymity and privacy are linked, their meanings are vastly different.

2. Explains Internet Privacy

Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Internet privacy risks include :

A. **Phishing :** An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.

B. **Pharming :** An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.

C. **Spyware :** An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.

D. **Malware :** An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Internet privacy violation risks may be minimized, as follows :

A. Always use preventative software applications, such as anti-virus, anti-malware, anti-spam and firewalls

B. Avoid shopping on unreliable websites

C. Avoid exposing personal data on websites with lower security levels

D. Clear the browser's cache and browsing history on a consistent basis

E. Always use very strong passwords consisting of letters, numerals and special characters

3. Risks to Internet privacy

Companies are paid to monitor which websites individuals visit and then utilize the data, such as delivering advertisements depending on one's surfing history. People can reveal personal

information in a variety of ways, including through the use of "social media" and by sending bank and credit card information to various websites. Furthermore, directly observed behavior, such as browsing logs, search queries, or Facebook profile contents, can be automatically processed to infer potentially more intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality.[1]. Furthermore, even without any previous behavioral data, tracking onsite user interaction can yield a large number of insights, such as post code, name, and local address.[2]

Those worried about Internet privacy often list a variety of privacy hazards — occurrences that may violate privacy — that can occur as a result of using the Internet. These activities vary from the collection of user statistics to more harmful activities such as the distribution of malware and the exploitation of different types of vulnerabilities (software faults).

Several social networking sites make an effort to protect their users' personal information. All registered users on Facebook, for example, have access to privacy settings, which allow them to prevent specific people from seeing their profile, choose their "friends," and limit who gets access to their photos and videos. Other social networking services, such as Google Plus and Twitter, include privacy options as well. When submitting personal information on the internet, the user may utilize these options.

Children and adolescents often use the Internet (including social media) in ways which risk their privacy : a cause for growing concern among parents. Young people also may not realise that all their information and browsing can and may be tracked while visiting a particular site, and that it is up to them to protect their own privacy. They must be informed about all these risks. For example,

---

1. *Kosinski, Michal; Stillwell, D.; Graepel, T. (2013).* "Private traits and attributes are predictable from digital records of human behavior". *Proceedings of the National Academy of Sciences. 110 (15) : 5802–5805.* doi :10.1073/pnas.1218772110. PMC 3625324. PMID 23479631.
2. *Matthees, Robert.* "Cross-Device Tracking : Advanced Client ID/Fingerprint User Identification". *www.robert-matthees.de.* Retrieved 2017-08-29.

on Twitter, threats include shortened links that lead one to potentially harmful places. In their email inbox, threats include email scams and attachments that get them to install malware and disclose personal information. On Torrent sites, threats include malware hiding in video, music, and software downloads. Even when using a Smartphone, threats include geolocation, meaning that one's phone can detect where they are and post it online for all to see. Users can protect themselves by updating virus protection, using security settings, downloading patches, installing a firewall, screening email, shutting down spyware, controlling cookies, using encryption, fending off browser hijackers, and blocking pop-ups.[3]

The privacy concerns of Internet users pose a serious challenge. In an online survey conducted, approximately seven out of ten individuals responded that what worries them most is their privacy over the Internet than over the mail or phone. Internet privacy is slowly but surely becoming a threat, as a person's personal data may slip into the wrong hands if passed around through the Web.[4]

4. Privacy issues of social networking sites

Web 2.0 has resulted in social profiling, which is a rising issue for Internet privacy. Web 2.0 is a system that allows people to share and collaborate on information on the internet via social networking sites like Facebook, Instagram, Twitter, and MySpace. Since the late 2000s, several social networking services have experienced a surge in popularity. Many individuals are disclosing personal information on the internet as a result of these websites.

5. Other potential Internet privacy risks

A. Malware is a term short for "malicious software" and is used to describe software to cause damage to a single

---

3. *Youn, S. (2009). "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents". Journal of Consumer Affairs. 43 (3) : 389–418.* doi :10.1111/j.1745-6606.2009.01146.x
4. *Larose, Robert; Choi, Hyunyi (November 1, 1999).* "Privacy Issues in Internet Surveys". *Social Science Computer Review. 17 (9).* doi :10.1177/089443939901700402

computer, server, or computer network whether that is through the use of a virus, trojan horse, spyware, etc.[5]

B. Spyware is a piece of software that obtains information from a user's computer without that user's consent.[6]

C. A web bug is an object embedded into a web page or email and is usually invisible to the user of the website or reader of the email. It allows checking to see if a person has looked at a particular website or read a specific email message.

D. Phishing is a criminally fraudulent process of trying to obtain sensitive information such as user names, passwords, credit card or bank information. Phishing is an internet crime in which someone masquerades as a trustworthy entity in some form of electronic communication.

E. Pharming is a hacker's attempt to redirect traffic from a legitimate website to a completely different internet address. Pharming can be conducted by changing the hosts file on a victim's computer or by exploiting a vulnerability on the DNS server.

F. Social engineering where people are manipulated or tricked into performing actions or divulging confidential information.[7]

G. Malicious proxy server (or other "anonymity" services).

H. Use of weak passwords that are short, consist of all numbers, all lowercase or all uppercase letters, or that can be easily guessed such as single words, common phrases, a person's name, a pet's name, the name of a place, an address, a phone number, a social security number, or a birth date.[8]

---

https ://technet.microsoft.com

Ibid.

"Social Engineering : The Basics".

I. Using the same login name and/or password for multiple accounts where one compromised account leads to other accounts being compromised.[9]

J. Allowing unused or little used accounts, where unauthorized use is likely to go unnoticed, to remain active.[10]

K. Using out-of-date software that may contain vulnerabilities that have been fixed in newer more up-to-date versions.

L. WebRTC is a protocol which suffers from a serious security flaw that compromises the privacy of VPN-tunnels, by allowing the true IP address of the user to be read. It is enabled by default in major browsers such as Firefox and Google Chrome.[11]

---

9. Digital Tools to Curb Snooping", Somini Sengupta, New York Times, 17 July 2013
10. Top 5 Online Privacy Tips". *Net-Security*. Retrieved 2012-11-23.
11. Huge Security Flaw Leaks VPN Users' Real IP-addresses TorrentFreak.com (2015-01-30). Retrieved on 2015-02-21

CHAPTER FIVE

E-commerce in Bangladesh

1. Introduction

E-commerce has become a buzzword in Bangladeshi information technology. It is the method of doing all types of business via a computer network and using digital communication. Increasing domestic and worldwide competition, the economic crisis, quickly changing market trends, and unpredictable financial markets have all increased the demand on businesses to devise effective solutions in order to survive and thrive. If we want to be a part of global company, e-commerce is one of the areas that need greater attention. Bangladesh is still a long way from adopting the main stream of e-commerce software. Furthermore, for organizations in emerging and rapidly industrializing countries like Bangladesh, lowering international trade barriers, economic liberalization, globalization, and deregulation have created a slew of new difficulties. As a result, a discussion of the benefits and drawbacks of e-commerce in Bangladesh is relevant. The government of Bangladesh has made steps to reinvent our internet technology and broadband network with a goal of "Digital Bangladesh." The article examines the advantages of e-commerce and how they influence the adoption of various forms of e-commerce in order to create digital transactions and companies, allowing nations' industries to deal with continuing problems.

E-commerce is becoming popular in Bangladesh. With better access, coverage and an ever-growing Netizen[1],[2], the prospect for e-

---

1. The term netizen is a portmanteau of the words Internet and citizen as in "citizen of the net". It describes a person actively involved in online communities or the Internet in general.
2. *'The Net and Netizens'* , Michael Hauben, Columbia University.

Commerce[3] is bright. The vast majority of the e-commerce businesses within Bangladesh are of C2C[4] (Consumer to Consumer). Some B2B[5] (Business to Business) and B2C[6] (Business to Consumers) have shown exponential growth prospects in recent years. This paper aims at examining whether there is any gap between the philosophy of the e-commerce and the reality in the developing countries like Bangladesh and identifies the factors lies behind this gap. Then this paper suggests some measures to be taken to minimize the gap.

2. E-commerce Concept

E-commerce is a narrower part of e-business dealing with the purchase and sale of goods and services over the internet, including support activities such as marketing and customer support.

The ability to made transaction for personal or professional use over the internet is known as electronic commerce or e-commerce. Chaffey (2007) defined e-commerce as *"The exchange of information across electronic networks, at any stage in the supply chain, whether within an Organization, between businesses, between businesses and consumers or between the public and private sector, whether paid or unpaid."*

3. Types of E-Commerce

Adam (2003) categorized e-commerce in 4 categories which are

i) Business-to-Business (B2B)

Business-to-business e-commerce deals between the businesses or among the businesses. Most of B2B applications are used in the

---

3. *E-commerce* is the activity of buying or selling of products on online services or over the Internet.
4. *Consumer to consumer*, or *C2C*, is the business model that facilitates commerce between private individuals.
5. Business-to-business (B2B) is a situation where one business makes a commercial transaction with another.
6. Business-to-consumer (B2C) is an Internet and electronic commerce (e-commerce) model that denotes a financial transaction or online sale between a business and consumer. B2C involves a service or product exchange from a business to a consumer, whereby merchants sell products to consumers.

area of distribution management, inventory management, channel management, supplier management and payment management.

ii) Business to-Consumer (B2C)

Business-to-Consumer ecommerce is involved between the businesses and the consumers. Most of B2C e-commerce deals with purchasing of physical goods like books or any consumer product, information goods like software, e-book, games, song etc., and personal finance management like e-banking

iii) Consumer-to-Consumer (C2C)

Consumer-to-Consumer e-commerce deals between individual consumers. Online auction and peer-to-peer system for money or file exchange could be the examples of C2C e-commerce. Business-to-Government e-commerce is involved between the business organizations and the government.

iv) Business-to-Government (B2G)

B2G is generally used for licensing process, public purchasing and other government operations. Though this type of ecommerce is insignificant compare to other kind of e-commerce, but it could be a driving force for operating public sectors which is refer as e-governance.

4. E-commerce Practice in Bangladesh

E-commerce in Bangladesh actually stated in the year of 1999 based in USA with some non-resident Bangladeshis. This people opened some Bangladeshi sites focused on providing local news and some transactional things like sending gift items to Bangladesh. www.munshigi. com is the first ever Bangladeshi e-commerce web site.

4.1 List of different e-commerce-type web sites are :

www.chorka.com,www.hutbazar.com,www.cellbazar.com,www.muktabazaar.com,www.bikroy.com,www.banglacommerce.com,www.bdjobs.com,www.premium.com,www.shoppingcard.com www.Ecommercebank.org,www.kroybikroy.com,www.kholabazar.com,www.bestway.com,www.sonalibangla.com,www.ebangla.com,w

ww.bajna.com,www.bangladeshinfo.com,www.bdbazar.com,www.b
dquery.com,www.quickezine.com,www.webbangladesh.com,www.d
eshigift.com,www.bangla2000.com,www.banglabaskets.com etc.

5. Challenges of E-commerce implementation in Bangladesh

Bangladesh's public electricity sector is woefully underdeveloped. Overloading and a lack of maintenance result in frequent outages and the need for scheduled blackouts. Telecommunications services in the country are poor. 60 percent of the lines are analog, and the service quality is poor; 30 percent of the lines are connected, and there is a lack of suitable commercial understanding and technical capabilities to set up e-commerce operations. There are insufficient trainers to educate E-commerce knowledge as well as government laws and regulations. Bangladesh's e-commerce policy is also insufficient for excellent results.

6. Barriers hindering e-commerce adoption in Bangladesh

The study identified specific infrastructural barriers hindering the adoption of e-commerce in Bangladesh. There is a wide range of reasons why ecommerce adoption in Bangladesh is hindered :

6.1 Infrastructural barriers

Some of the barriers include lack of credit cards[7] (the wide availability of them for the general public in developing countries) and convenient payment means, poor distribution logistics, lack of specialized, trust-worthy online merchants of reasonable size, imperfect legal system, and lack of large scale telecommunication transmission capability (broadband), Internet security", "lack of feel-and-touch associated with online purchases", "problems in returning products", and "selection" (product availability and breadth).

---

7. A credit card is a payment card issued to users (cardholders) to enable the cardholder to pay a merchant for goods and services based on the cardholder's promise to the card issuer to pay them for the amounts plus the other agreed charges.

6.2 Technology

There are serious infrastructural challenges in Bangladesh. This research identified various infrastructural characteristics as barriers hindering ecommerce adoption in Bangladesh. Among the most pressing infrastructure limitations are access to technology[8] , limited bandwidth, which reduces the capacity to handle audio and graphic data; poor telecommunications infrastructures[9] and unreliable electricity supply.

6.3 Telecommunication (network)

E-commerce success relies heavily on a number of technology infrastructures. Telecommunication infrastructures are required to connect various regions and parties within a country and across countries. In the absence of an adequate basic infrastructure, it is possible that the potential advantages of the use of electronic commerce turn into disadvantages. In the case of telecommunications for example, where the infrastructure is not at the same level of development in all regions of the world, access to the Internet in most developing countries like Bangladesh is very slow and expensive.

6.4 High access cost

The cost of the Internet access makes it inaccessible to most users in Bangladesh. The cost of accessing the infrastructures also influences the growth of ecommerce. The priority for most developing countries is to put in place the necessary infrastructure and a competitive environment and regulatory framework that support affordable Internet access. The monthly connection cost of the Internet far exceeds the monthly income of a significant portion of the population.

Internet access prices are a key determinant of Internet and ecommerce use by individuals and businesses. Countries with lower access costs typically have a greater number of Internet hosts, and

---

8. Computers, connectivity, and gateway to Internet.
9. Most of which are still analogue and can only transmit voice.

electronic commerce has developed rapidly in countries with unmetered (flat-rate) access. The basic network infrastructure must be in place for developing countries to participate in global ecommerce, although the development of reliable fixed communication networks is an important policy area for e-commerce, especially in Bangladesh.

6.5 Access to computer equipment

A combination of these costs and the high fees charged by telephones companies both contributed to discouraging Internet connectivity in developing countries and their participation in ecommerce. The necessary infrastructure for such widespread usage simply does not yet exist. Before computer technologies and the Internet in particular, can be used to assist Bangladesh to overcome their problems, the necessary infrastructure and deregulation need to be firmly in place. However, even with access to the necessary equipment, users will not become active ecommerce participants unless they have reasonable confidence in the integrity of transactions undertaken on- line. The presence of an adequate Internet infrastructure is a necessary but not sufficient condition for the development of ecommerce.[10]

6.6 Socio-cultural barriers

Most cultures in Bangladesh do not support ecommerce and the conditions are not "ripe" because of lack of confidence in technology and online culture (Efendioglu et al, 2004). The social and cultural characteristics of most developing countries and the concepts associated with online transaction pose a much greater challenge and act as a major barrier to adoption and diffusion of ecommerce. Even though online transaction that are pre-cursors to e-commerce, such as catalog and telephone sales, have existed in developed countries and have been used by the public for an extended time period

---

10. Joanne E. Oxley, Bernard Yeung '*E-Commerce Readiness : Institutional Environment and International Competitiveness*' Journal of International Business Studies, December 2001, Volume 32, Issue 4, p.p 705–723.

(Efendioglu et al, 2004), such systems are new and novel approaches in developing countries and is not suitable to the culture and way of doing business. Since the business foundation of ecommerce is based on such a methodology, some of these local cultural characteristics do pose significant challenges for the e-commerce adoption. The researcher identified various socio-cultural characteristics as barriers hindering ecommerce adoption in Bangladesh. Among the most pressing primary cultural barriers are level of trust in institutions, shopping as a social place, limitation on personal contact and language/content.

6.7 Limitation on personal contact

The adoption of e-commerce depends on the cultural and social environment. In most developing countries, people consider shopping as a recreational activity (Boerhanoeddin, 2000). The idea of buying goods that one cannot see and touch and from sellers thousands of miles away may take some "getting used to" for those who are used to face-to-face transactions, familiarity with the other party, (strong individual relationship and long term association between the parties), and getting satisfaction from winning business negotiations (they are willing to employ a variety of tactics to get the best deal). As one person stated "I like buying over the Internet, but it does not beat going to an actual shop where you can see what you are buying and make sure it's what you want" (Lawrence, 2002). All of these long standing cultural traits are undermined by and are contrary to the depersonalization associated with ecommerce and business systems designed to sell products online in Bangladesh.

6.8 Political and Governmental Barriers

The poor state of most developing countries telecommunications infrastructure is the major barriers hindering the adoption of ecommerce. The lack of telephone lines, low quality, slow speed and high cost of bandwidth and security concerns needs to be addressed before users and enterprises in Bangladesh can think of participating in ecommerce.

It is very crucial in developing countries Governments to ensure open and competitive telecommunication markets that offer a range of interoperable technological options and network services (particularly broadband) of appropriate quality and price, so that users can choose among various technologies and services for high-speed Internet access. Other issues that are seen as barriers to ecommerce adoption are free trade, the monopoly which national governments exercise over national telecommunications, import duties on IT equipment like hardware and software. The elimination of control and deregulation of telecommunication systems is necessary before a free flow of information and an expanded use of ICT is possible. Changes in government policy are perceived as being critical to creating an environment for the broad use of the Internet in many sectors of Bangladesh.

The conditions in most developing countries are sadly not conducive to the widespread, cheap and effective use of the Internet by the majority of citizens. There is neither a government policy on Internet provision or on the future of ecommerce in most developing countries nor any comprehensive information policy. The absence of national information policies in developing countries means that the government is not involved in Internet provision.

7. Policy Required/ Recommendations

E-commerce sector brings enormous opportunities to the business sector as it makes 24/7 business possible. It makes the economic activities more dynamic. E-commerce can play important role in achieving expected economic growth and socio-economic development. E-commerce has been successful in increasing GDP[11]. In order to obtain sustainable economic development as well as business growth Bangladesh government should flourish e-commerce. With regard to e-commerce Bangladesh needs to maintain some effective steps.

---

11. GDP is the final value of the goods and services produced within the geographic boundaries of a country during a specified period of time, normally a year. GDP growth rate is an important indicator of the economic performance of a country. Available at https ://economictimes.indiatimes.com/definition/gross-domestic-product.

The followings are some of the recommendations that will ensure the smooth functioning as well as the widespread use of e-commerce in Bangladesh.

Bangladeshi e-commerce sites should provide greater layers of security for their payment procedures. The government should provide the necessary support to e-CAB[12] (E-commerce Association of Bangladesh) so more people can be trained in this sector. E-commerce businesses require high-speed internet, which is absent in the rural areas. The government should take the internet as a fundamental element of business, particularly e-commerce business. It must ensure low-cost, high-speed internet for rural people to turn its vision of Digital Bangladesh into reality. Bangladeshi e-commerce sites should not only update and evolve, but also address the growing concerns like managing increased visits and purchases during the holidays, payment methods.

Effective IT security system should maintain by adopting latest IT technology. Bangladeshi e-commerce sites should aim to improve customer service and address areas of concern to reach out to the part of the population which is not opting for e-commerce yet.

Fashion and electronic products are currently dominating the e-marketplace; products of e-marketplace should be diversified. To penetrate into the global market, the government has to reform its regulations regarding online transactions and upgrade the entire system.

The Bangladesh Bank[13] should formulate policies to ease the loan process for e-commerce entrepreneurs. The government should do something about providing trade license[14] for e-commerce businesses. Currently, trade license is not issued specifically for e-

12. E-commerce Association of Bangladesh.
13. Bangladesh Bank, the central bank and apex regulatory body for the country's monetary and financial system, was established in Dhaka as a body corporate vide the Bangladesh Bank Order, 1972 (P.O. No. 127 of 1972) with effect from 16th December, 1971.
14. Trade License is a license or permission issued by the municipal corporation granting permission to carry on a particular trade on a particular address.

commerce businesses, which makes running such businesses difficult. It is important for Bangladesh to update the ICT law[15] relating to e-commerce. It should be done focusing on international practices.

8. Conclusion

Although a few numbers of people in our country getting the benefits from e-commerce, development of e-commerce in our country must have strongly reflects on livelihood. By flourishing this potential sector all people of our country will be benefited. E-marketplace[16] is a store of information which acts as information agent that provides buyers and sellers with information on products. To increase participant of online shopping, the sources of consumer confusion, apprehension and risk need to be identified, understand and alleviate. It can be concluded that through adopting e-commerce intensively and extensively businessmen can improve their income level along with improvement of customer satisfaction and buyer can reduce their cost of living along with improvement of their standard of living.

15. Act no 39 of 2006
16. E-market place is a virtual online market platform where companies can register as buyers and sellers to conduct business to business transactions over the internet.

CHAPTER SIX
E-Contract

The Law of Electronic Contracts in Bangladesh

1. Introduction :

One of the branches of e-business is e-contract. It has a similar connotation to conventional commerce, in which products and services are exchanged for a certain sum of money. The only difference is that the contract is executed through a digital means of communication such as the internet. It allows merchants to reach out directly to the end user without the need for a middleman.[1]

Different organizational charters are required for new company models. E-contract necessitates an organizational charter that addresses its new marketing requirements. Businesses may save time on product design and create goods based on specific client requirements, monitor sales, and get instant feedback from customers using this business model.

There was initially apprehension among legislators about recognizing this contemporary technology, but many nations now have legislation in place to accept electronic contracts. The traditional contract law does not adequately handle all of the problems that emerge with electronic transactions. The Information Technology Act explains how to create and verify electronic contracts and addresses some of the problems that may emerge.

In reality as per observation it can be said that across lack of provision in formation of e-contract. Information Communication and Technology Act[2], Cyber Law, Contract Act[3], Evidence Act[4] not

---

1. Richard Duncombe, Richard Heeksn et al., Ecommerce for Small Enterprise Development 204 (2006)
2. Act no 39 of 2006.
3. Act no ix of 1872.
4. Act no I of 1872.

wholly justified to electronic contract. Today's computerized generation[5] need more protection. Our Bangladeshi judiciary in many landmark judgments' rejected legality of computer. Then it's very difficult to define even justified validity of electronic contract. It often come across these e-contracts in our day to day life but is unaware of the legal complexities and challenges connected to it.

2. Definition of E-Contract :

Any contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means, such as e-mail, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract is referred to as an e-contract. E-contracts are subject to the same contract principles and remedies as traditional contracts. This is sometimes referred to as a "electronic contract."

According to Sir William Anson *'A contract is a legally binding agreement between two or more persons by which rights are acquired by one or more acts or forbearance on the part of the other or others'*. E-contract is any kind of contract formed in the course of e-commerce[6] by the interaction of two or more individuals using electronic means, such as e-mail[7], the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract. Traditional contract[8] principles and remedies also apply to e-contracts. This is also known as

---

5. *Generation* in *computer* terminology is a change in technology a *computer* is/was being used. Initially, the *generation* term was used to distinguish between varying hardware technologies. Nowadays, *generation* includes both hardware and software, which together make up an entire *computer* system.
6. *Ecommerce*, also known as *electronic commerce* or internet *commerce*, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions
7. Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.
8. a legal document that states and explains a formal agreement between two different people or groups, or the agreement itself.

electronic contract. E-Contract is an aid to drafting and negotiating successful contracts for consumer and business e-commerce and related services. It is designed to assist people in formulating and implementing commercial contracts policies within e-businesses.[9] It contains model contracts for the sale of products and supply of digital products and services to both consumers and businesses.

E-contract is a contract modeled, executed and enacted by a software system. Computer programs are used to automate business processes that govern e-contracts. E-contracts are conceptually very similar to traditional (paper based) commercial contracts. Vendors[10] present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payments. Then, the vendors deliver the purchased products. Nevertheless, because of the ways in which it differs from traditional commerce, electronic commerce raises some new and interesting technical and legal challenges.

3. Essentials of an electronic contract

As in every other contract, an electronic contract also requires the following necessary requirements :

3.1. An offer requirements to be made

In many contacts (whether online or conventional) the offer is not made directly one-on-one. The consumer 'browses' the available goods and services showed on the seller's website and then choose what he would like to purchase. The offer is not made by website showing the items for sale at a particular price. This is essentially an

---

9. Electronic *business* (*e-business*) refers to the use of the Web, Internet, intranets, extranets or some combination thereof to conduct *business*. *E-business* is similar to *e*-commerce, but it goes beyond the simple buying and selling of products and services online. Available at : https :// www.techopedia.com/definition/1493/electronic-business-e-business.
10. A *vendor*, or a *supplier*, is a supply chain management term that *means* anyone who provides goods or services to another entity. *Vendors* may sell B2B (business-to-business; i.e., to other companies), B2C (business to consumers), or B2G (business to government).

invitation to offer and hence is revocable at any time up to the time of acceptance. The offer is made by the customer on introduction the products in the virtual 'basket' or 'shopping cart' for payment.

3.2. The offer needs to be acknowledged

As stated earlier, the acceptance is usually assumed by the business after the offer has been made by the consumer in relation with the invitation to offer. An offer is revocable at any time until the acceptance is made.

Processes available for forming electronic contracts include :

I. E-mail : Offers and acceptances can be exchanged entirely by e-mail, or can be collective with paper documents, faxes, telephonic discussions etc.

II. Web Site Forms : The seller can offer goods or services (e.g. air tickets, software etc.) through his website. The customer places an order by completing and communicating the order form provided on the website. The goods may be actually delivered later (e.g. in case of clothes, music CDs etc.) or be directly delivered electronically (e.g. e-tickets, software, mp3 etc.).

III. Online Agreements : Users may need to take an online agreement in order to be able to avail of the services e.g. clicking on "I accept" while connecting software or clicking on "I agree" while signing up for an email account.

3.3. There has to be legal consideration

Any contract to be enforceable by law must have legal consideration, i.e., when both parties give and receive something in return. Therefore, if an auction site eases a contract between two parties where one Ecommerce – Legal Issues such as a person provides a pornographic movie as consideration for purchasing an mp3 player, then such a contract is void.

3.4. There has to be an intention to create lawful relations

If there is no intention on the part of the parties to create lawful relationships, then no contract is possible between them. Usually, agreements of a domestic or social nature are not contracts and therefore are not enforceable, e.g., a website providing general health related data and instructions.

3.5. The parties must be able to contract

Contracts by minors, lunatics etc. are void. All the parties to the contract must be lawfully competent to enter into the contract.

3.6. There must be free and unaffected consent

Consent is said to be free when there is absence of coercion, misrepresentation, undue influence or fraud. In other words, there must not be any agitation of the will of any party to the contract to enter such contract. Usually, in online contracts, especially when there is no active real-time communication between the contracting parties, e.g., between a website and the customer who buys through such a site, the click through process ensures free and genuine consent.

3.7. The object of the contract needs to be lawful

A valid contract presumes a lawful object. Thus a contract for selling narcotic drugs or pornography online is void.

3.8. There must be conviction and possibility of performance

A contract, to be enforceable, must not be ambiguous or unclear and there must be possibility of performance. A contract, which is impossible to perform, cannot be enforced, e.g., where a website promises to sell land on the moon.

4. Types of Electronic Contracts

4.1. Employment Contracts

The Information Technology is determined by manpower in Bangladeshi context and thus employment contracts are vital. With high erosion rate as well as the confidentiality involved in the work

employment contracts become crucial. Apart from that Bangladeshi Labour practices are based on tough labour laws and not the hire and fire processes of the first world. In this background copyright issue of software development assumes vital importance. Apart from that contracts for on-site development and sending the workforce abroad and security clauses will play a crucial role in employment contracts. Firms hiring personnel abroad apart from their personnel need to include the relevant employment contract of the place of action.

4.2. Consultant Agreements

The normal requirements of the Contracts Act of 1872 will apply on any consultant agreement. But particularly in Information Technology industry where the infrastructure to function is low and connectivity is very high consultancy with experience marketing and business development and technology development is a very dominant mode of contract. Here proper care to be taken in Consultant agreements where issues of Intellectual Property Rights, privacy will play an important role. If care is not taken it may lead to cost of business and loss of clients.

4.3. Contractor Agreements

As manufacturing companies subcontract their business, Information Technology also subcontract their work due to changing orders and would like to cut on the cost of regular workforce and attendant legal and financial problems. Here again privacy, consumer liability and copy right issues assume great importance and care to be taken in representation such contracts.

4.4. Sales, Re-Seller and Distributor Agreements

In software and Internet dealings though the order of middle men are done away with, it still requires a circulation network and hence prescribed issues come into play in that feature of business. In first place one needs to see whether software is a good in the Sale of Goods Act.

Software is a programme of instructions, which operate the system or hardware to function in a planned manner. Hence there

arises an effort to classify and define in legal terms of the vague nature of software in comparison with other products. The code and its source can be understood as information planned in a way to operate the system leading to the conclusion it is not a property and not a good in the legal intellect. In *Aerodynamics Systems Product* v. *General Automation limited*, the argument upraised by the defendants that though software can be a subject matter of sale, software them self is pure information, and the transmission of software is a service and not sale of goods. There is another explanation of Software to be considered as Goods where it is likened to that of a book containing information, which is considered as goods under the Sale of Goods Act. As the value of the book is not the mere value of the inlet jacket, paper and materials used in its creation, but one that of the value of the information limited in it, software is also a product –a floppy, or a CD-ROM or simply stored in hard disc but the value is much higher than the simple storage device.

Hence software due its high value in terms of application is measured as goods for the purpose of legal classification. Having recognised it as good the distribution, reseller agreement should take care of the aspect of Monopoly Restrictive Trade Practices (in future the competition law) provincial authority and other tax instruments.

4.5. Non-Disclosure Agreements

Non-Disclosure Agreements are part of IT contracts, which identify binding agreements with employees apart from the standard confidentiality agreements. The Contract Act 1872 has provisions for the same and it undertakes importance in an industry which is purely knowledge based and one which can be easily repeated ruining the business.

4.6. Software Development and Licensing Agreements

A license is an authorisation given to do a specific manufacture/sales/marketing/distribution, which is legitimate. License plays a prevailing form of contract in mass marketing activity of any kind including Information Technology. Software

licensing has a historical background where originally it was pushed with the hardware and was given free and its use and application was limited to that of operating the system and few other features.

4.7. Shrink Wrap Contracts

A Shrink Wrap contract is the former license agreement required upon the buyer when he buys software. Before he or she tears the pack to use it, he or she is made mindful by tearing the cover or the wrap that they are sure by the license agreement of the manufacture. This is done as previous deliberated to protect the interests of the manufacturer where the consumer cannot replicate the package, copy it or sell it or donate it to others moving the sale of the software. The license, which is contracted and enfolded in the product, which becomes enforceable and taken as consent before the buyer tears the package. The usual sections that are part of the shrink-wrap license are that of

a) prohibiting illegal creation of copies
b) prohibiting payments of the software
c) prohibition of contrary engineering, de-compilation or adjustment
d) prohibition of usage in more than one computer definite for that purpose
e) disclaimer of contracts in respect of the product sold
f) limitations of responsibility

The reason and business sense is that to guard the manufacturer of the package, as it is easy to copy, operates and duplicate under other brand name. Critiques contend that shrink-wrap license agreement is in contradiction of the basic principle of contract of offer, consideration and acceptance as the licensee is unsettled. Several cases to this effect have been dispensed in US courts.

4.8. Source Code Escrow Agreements

In software development many principal firms who participate in development are keen to guard the source code of the software, which is the most appreciated and cautious part of the computer programme. Copyright owners of such source code may have to

disclose this to countless developers who will be developing definite software based on the source code. In these conditions, the copyright owner will credit the source code to specified source code escrow agents who will release the code on the development of the product upon agreed terms. In cyber contracts, such agreements and also the terms and conditions to contract with the escrow agents become vital.

5. Recognition of E-contracts

For Recognition of e-contracts following questions are needed to be considered

1. Whether e-contract is a valid contract?
2. Would a supplier makes details of goods and services with prices available on a website be deemed to have made an offer?
3. Whether e-contracts satisfy the legal requirements of reduction of agreements to signed documents.
4. Whether e-contracts interpret, adopt and compile the other existing legal standards in the context of electronic transactions?

A. Offer : The law already recognizes contracts formed using facsimile, telex and other similar technology. An agreement between parties is legally valid if it satisfies the requirements of the law regarding its formation, i.e. that the parties intended to create a contract primarily. This intention is evidenced by their compliance with 3 classical cornerstones i.e. offer, acceptance and consideration. One of the early steps in the formation of a contract lies in arriving at an agreement between the contracting parties by means of an offer and acceptance. Advertisement on website may or may not constitute an offer as offer and invitation to treat are two distinct concepts. Being an offer to unspecified person, it is probably an invitation to treat, unless a contrary intention is clearly expressed. The test is of intention whether by supplying the information, the person intends to be legally bound or not. When consumers respond through an e-mail or by filling in an online form, built into the web page, they make an Offer. The seller can accept this offer either by express confirmation or by conduct.

B. Acceptance : Unequivocal unconditional communication of acceptance is required to be made in terms of the offer, to create a valid e-contract. The critical issue is when acceptance takes effect, to determine where and when the contract comes into existence. The general receipt rule is that acceptance is effective when received. For contracting no conclusive rule is settled. The applicable rule of communication depends upon reasonable certainty of the message being received. When parties connect directly, without a server, they will be aware of failure or partial receipt of a message. Such party realizing the fault must request re-transmission, as acceptance is only effective when received. When there is a common server, the actual point of receipt of the acceptance is crucial in deciding the jurisdiction in which the e-contract is concluded. If the server is trusted, the postal rule may apply, if however, the server is not trusted or there is uncertainty concerning the e-mail's route, it is best not to apply the postal rule. When arrival at the server is presumed insufficient, the 'receipt at the mail box' rule is preferred.

C. Consideration and Performance : Contracts result only when one promise is made in exchange for something in return. This something in return is called 'consideration'. The present rules of consideration apply to e-contracts. There is concern among consumers regarding Transitional Security over the Internet. The e-directive on Distance Selling tries to generate confidence by minimizing abuse by purchasers and suppliers. It specifies–

a) A list of key points must be supplied to the consumer in 'a clear and comprehensible manner.'

b) Written confirmation, or confirmation in another durable medium available and accessible to the consumer, of the principle points.

c) The right of withdrawal enabling consumers to avoid deals entered into inadvertently or without sufficient knowledge, providing for seven-day cooling-off period free from penalty or reason to return the goods or reimburse the cost of services.

d) Performance should be delivered within thirty days of order unless otherwise expressly agreed.

e) Reimbursement of sums lost to fraudulent use of credit cards. It places the risk of fraud on the credit card Company, requiring them to take steps to protect their position.

f) On the other hand, there is also need to protect sellers from rogue purchasers. For this, the provision of 'charge-back clauses' and encouragement of pre-payment by buyers is recommended.

g) Thus, this Directive adequately protects rights of consumers against unknown sellers and sellers against unknown buyers.

D. Liability and Damages : A party that commits breach of an agreement may face various types of liability under contract law. Due to the nature of the systems and the networks that business employ to conduct e-commerce, parties may find themselves liable for contracts which technically originated with them but, due to programming error, employee mistake or deliberate misconduct were executed, released without the actual intent or authority of the party. Sound policies dictate that parties receiving messages be able to rely on the legal expressions of the authority from the sender's computer and this legally be able to attribute these messages to the sender.

In addition to employing information security mechanisms and other controls, techniques for limiting exposure to liability include :

1. Trading partner and legal technical arguments
2. Compliance with recognized procedures, guidelines and practices
3. Audit and control programmers and reviews
4. Technical competence and accreditation
5. Proper human resource management
6. Insurance
7. Enhance notice and disclosure mechanisms and
8. Legislation and regulation addressing relevant secure electronic commerce issuing.

6. Legal Framework Relating to E-contract

With the growing importance and value of e-contract in Bangladesh and across the world, the different stakeholders are continuously identifying and evaluating the nuances of legal outline relating to it. The participation of different service providers in the transaction of e-contract, which includes a payment gateway, the main website, the bank or card verification website, the security authorisation website and the final service provider which can also comprise the shipping agent has made the E-contract business more complex. Therefore, the need for amendable it has augmented. In India, till date there are no definite legislations or guidelines protecting the buyers and sellers of goods and services over the electronic medium.[11] However, several laws acting in unification are trying to regulate the business transactions of E-contract. They are as follows :

1. Contract Act,1872
2. The Consumers' Right Protection Act,2009[12]
3. Information Communication and Technology Act,2006
4. The Copyright Act,2000[13]

Like any other types of business, E-contract business also works on the basis of contracts. It is therefore, structured by the Contract Act, 1872. Any valid and legal E-contracts can be designed, completed, and enforced as parties replace paper documents with electronic parallels.[14] The contracts are move in between the service providers or sellers and buyers.

The authority of the transactions of E-contract is established under the Information Communication and Technology Act, 2006. It explains the reasonable mode of acceptance of the offer. This Act also rules the revocation of offer and acceptance.[15] However, definite provisions that regulate E-contract transactions conducted over the internet, mobile phones, etc. are vague. With numerous cross border

---

11. Akshat Razdan, *The Future of E-Commerce in India*, LAW WIRE
12. Act no 26 of 2009.
13. Act No. XXVIII of 2000.
14. Aashit Shah & Praveen Nagre, *Legal Issues in E-commerce*
15. Vikas Asawat, *Information Technology (Amnedment) Act, 2008 : A New Vision through a New Change*

transactions also being conducted over the internet, specific law guarding the Indian customers and Indian businesses are essential and Indian laws are gravely insufficient on this issue.

In a bid to safeguard security, the government has made digital signatures necessary in several E-contract transactions mainly in the government to government (G2G) or government to business (G2B) framework with a view to safeguarding the identity of the transacting parties. E-contracts transactions on these modes require digital signatures as essential parts. They are used for the verification of the electronic contracts. These are controlled by the ICT Act, 2006 which provides the outline for digital signatures, their issues and verification. The Act thus tries to safeguard that trust between both the parties is maintained through verification of identities and help prevent cybercrimes and ensure cyber security practices.[16]

In the light of the above discussion, it is to be said that the present laws in respect of the guidelines of E-contract and its related operations are not suitable serving the purpose. Propagation of laws is creating confusion in the smooth procedures of the E-contract accomplishments. Further, the present laws are salient on features of e-contract such as payment instrument and delivery instrument and present standard practices which have been settled by the industry. The Bangladesh Bank[17], however, has tried to support the electronic payment mechanism through various orders, but such orders can only act as a stop-gap procedure.[18] The most important order in this regard was the application of second factor verification in Bangladesh Payment Gateways. Commonly recognised as verified by Visa[19] or Master Card [20]Secure Code, this had made card transactions on the internet moderately more secure.

---

16. Dr. Shuchi Singhal, *Digital Signatures : Bringing a Paradigm Shift in E-Banking*, 5(1) Pacific Business Review International 61,62 (2012).
17. The Central Bank of Bangladesh
18. Bienu Vaghela, *RBI Secures online credit and transaction*, Business Standard
19. A card that bears the Visa symbol and which enables a Visa cardholder to obtain goods, services or cash from a Visa merchant or acquirer, and have the transaction processed through its network. Visa does not itself issue credit or debit cards, but partners with card-issuing financial institutions.
20. MasterCard is a global bank card payment transaction processor, whose portfolio of brands and products include Maestro, Cirrus and MasterCard PayPass. It partners with financial institutions that issue credit cards, and with merchants who accept those cards.

7. Global Scenario in Respect to E-Contract

New intimidations to consumer protection call for new protecting rules and measures. We should distinguish the fact that better consumer protection in online environments shall have an optimistic impact on the further development of electronic commerce and thereby on merchants. Generally speaking, if electronic commerce is to increase, consumers must be provided with at least the same guarantees they would be provided with in the older marketplace.

The US[21] and the EU[22] have affirmed the importance of protecting a new type of consumers. With the rise of electronic commerce, the role of consumers has changed affectedly. While consumers were formerly a quiet body, today they have power in businesses. Sellers are now in a comparatively submissive position. Their job is too merely to paste that product information it becomes the accountability of consumers to evaluate and make active decisions upon.

Where the precise field of argument firmness is concerned, both the US and the EU realize the best way to safeguard consumers could be to provide them with suitable measures for recompense. Consumer protection groups have created mediums where consumers can both acquiesce e-mail based complaints when discontented with advertisements, goods or services, and allege violators of self-regulatory codes of beliefs.

While consumer protection can take on diverse forms, dispute resolve mechanisms are its final insurance. Principles for dispute management are finally more attractive to devices than less formal intended arrangements since they can encourage more reliable conduct of consumer benefits. In light of government practise, protection accessible by state power is important. Some consumers even seek reserve in the court. In order to quarter the special

---

21. The United States of America (USA), commonly known as the United States (U.S. or US) or America.
22. The European Union (EU) is a political and economic union of 27 member states that are located primarily in Europe.

character of modern business without drifting too far from tradition, ADR[23] mechanisms for dispute firmness very cleverly entail state application support. Procedure for consumer protection in electronic commerce dispute firmness must extend outside national limits. Individual states privation the ability and initiative to adequately address issues related to consumer protection in the background of electronic market. Many of the issues that arise from cross border disputes are impaired by the fact that misleading marketing practice laws vary from one jurisdiction to alternative. Possible standard electronic consumer policies should be pertinent to cross-border dealings to which all or most countries can subscribe.

OECD[24] Member States have acknowledged the necessity of an international synchronized approach to deal with the issue of dispute firmness in electronic business. In one imperative document framed by the OECD, Procedures for Consumer Protection in the Context of Electronic Commerce, procedures for consumer protection in dispute firmness and amends aim to safeguard consumers contributing in electronic business without founding barriers to trade.

The rules serve as a reference to governments, businesses, consumers, and their councils of the characteristics of active consumer protection for electronic business. The rationale behind them is alike to that of the US and EU. Firstly, applicable law and jurisdiction are singled out for likely amendment.

No broad creation of the new applicable law or principle of jurisdiction is pointed out, but the rules do define features of suitable modifications. Equality, they suggest, is one of the most important features in understanding consumer safety. The purpose of the

---

23. Alternative dispute resolution (ADR), or external dispute resolution (EDR), typically denotes a wide range of dispute resolution processes and techniques that act as a means for disagreeing parties to come to an agreement short of litigation : a collective term for the ways that parties can settle disputes, with the help of a third party. However, ADR is also increasingly being adopted as a tool to help settle disputes alongside the court system itself.

24 The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental economic organisation with 36 member countries, founded in 1961 to stimulate economic progress and world trade.

fairness is to offer consumers a level of protection not less than that afforded in other forms of commerce and to provide consumers with eloquent contact to fair and timely dispute resolution and redress without undue cost or burden. To complete fairness, one must provide a framework for correcting unfairness.

As said in the guidelines, businesses, consumer councils, and governments should work collected to endure to use and develop fair, effective, and clear self-regulatory and other measures, which provide consumers with the choice of mechanisms to firmness their disputes ascending out of consumer dealings. Moreover, these efforts should be followed at an international level. To attain the maximum reimbursements of the new arrangements, modern technology should be used to improve consumer awareness and freedom of choice. From the breakdown above, we can determine that the international community has touched a harmony on the general approach toward consumer protection. While making developments on court procedures and the application of principles, new means should be found out to quarter the new needs of electronic business. The means should permit the expansion of new shops effective in a responsible manner and resolving disputes accessibly online and, along with them, greater choices and more antagonism. With new services in place, consumers shall positively be protected from excessive costs of defiance with duplicative or varying guidelines.

8. Challenges of E-contracting in Bangladesh

8.1. Traditional Challenges :

Some issues indicate it will be challenges in forming e contracting in Bangladesh like Discoveries, Inventions and spread of new Information Technologies brought about by computers, internet and cyberspace widen the scientific horizon but pose new challenges and created problems for the legal world in all aspects of law. The challenges that Bangladesh facing today are not just confined to any single traditional legal system but in almost all major categories of law such as contract law, criminal law, Law of torts etc.

In Bangladesh, The information Communication and Technology Act, 2006 (ICT) and amendment in several existing laws

through ICT does enforce and control a level of cyber related problems. However, it has shown inadequacy of law while dealing with information technology itself. The ICT in many ways falls short of International standards. Therefore, in the era of information technology such loopholes in legal framework cannot be ignored and can lead to some impairment for individual as well as nation. New provisions added through Information communication and Technology (Amendment) Act, 2013 could be a way out from all these challenges but several changes are still needed for the act to ensure both functional equivalence and technological neutrality. Hence, there is an urgent need to redefine the cyber laws in Bangladesh as per International standards. There are few major areas in cyberspace in which many challenges have been cropped up on legal front. These areas are inherent challenges, legal challenges, technological challenges, political and social challenges, practical challenges etc.

8.2. Inherent Challenges

In many countries the laws related to cyberspace have already been developed. U.S. and the West drafted their own legislations by either adapting their existing laws in the context of cyberspace or creating new laws in respect thereof. Determining jurisdiction and formation of e-contracts are two key issues on which traditional legal principles have been largely applied by Bangladeshi Courts enacted its first law on ICT through the ICT Act, 2006 based on the principles Elicit dated in the UNCITRAL[25] Model law of e-commerce. It extends to whole of Bangladesh and also applies to any offence or contravention there under committed outside Bangladesh by any person.

---

25. The United Nations Commission on International Trade Law (UNCITRAL), established by the United Nations General Assembly by resolution 2205 (XXI) of 17 December 1966, plays an important role in developing that framework in pursuance of its mandate to further the progressive harmonization and modernization of the law of international trade by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law. Available at : https ://uncitral.un.org/.

8.3. Legal Challenges

a) Jurisdiction -Jurisdiction is the authority of a court to hear a case and resolve a dispute. The issue of Jurisdiction is highly conflicting and debatable in cyber law as to the maintainability of any suit which has been filed. It becomes more complicated largely on account of the fact that the internet is borderless. The notion of jurisdiction is rooted in territoriality from the point of view of both the court which can properly assert jurisdiction and from the point of view of the law that should be applied while deciding the dispute. In domestic transactions, a court will always have the jurisdiction to enforce their respective laws within their physical, geographical and political boundaries but the enforcement issues throws up several challenges when it comes to international transactions due to constant change in technology in borderless cyberspace. There have been various principles and test that lay down by the court in U.S. and U.K. which elaborated the scope of jurisdiction and the same is being followed by the Bangladeshi Court. However, the act still does not deal with some major legal issues such as Jurisdiction, protection of domain name, infringement of copyright law etc. This led the formation of various challenges before Bangladeshi Legal system.

9. Statutory effect of E-contract

The Contract Act, 1872 gives a statutory effect to the basic common law contractual rule that a valid contract may be formed if it is made by free consent of the parties, competent to contract, for a lawful consideration and for a lawful object and which is not void ab initio.[26] In general contract, the acceptor can revoke acceptance of the offer before it comes to the knowledge of the offeror, but what would be the case where an acceptance is sent via an electronic record, it may not be possible for the acceptor to revoke it before it comes to the knowledge of the offeror. However, there may be one possibility where revocation may still take place i.e. when the

---

26. A purported legal status or legal document that is taken to have never been valid or enforceable. from the start, from the moment of its purported existence.

acceptance is sent by an electronic record and the same is sent to a computer resource which is not the designated computer resource of the offeror, but it is not clear what would prevail when both the acceptance-revocation are retrieved by the offeror at the same time. Indian courts following the traditions of common law have developed the doctrine of "last-shot rule". This cardinal rule states that an acceptance should be unqualified and absolute and any acceptance even with little variation is no acceptance at all. The Contract Act does not prescribe or favor any particular way of communicating offer and acceptance. It may be done by word of mouth, writing or even by conduct. Thus; there is no requisite of writing for the validity of contracts except for cases which are specifically required by law to be in writing. Therefore, it would appear that the ICT Act avoids incorporating any specific provision giving validity to online contracts.

10. Jurisdictional problems in e-contracting in cyberspace

Legal validity of E-Contract -Electronic contracts are governed by the basic principles elucidated in the Contract Act, 1872,which mandates that a valid contract should have been entered with a free consent and for a lawful consideration between two adults. It also finds recognition under ICT Act, 2006 that provides validity to e-contracts. Accordingly, Contract Act, 1872and Information Communication and Technology Act, 2006 needs to be read in conjunction to understand and provide legal validity to e-contracts. Further, provisions of the Evidence Act, 1872 also provides that the evidence maybe in electronic form.

The Contract Act 1872 and The Evidence Act 1872 recognizing the validity of e-transaction has held that e-mails exchanges between parties regarding mutual obligations constitute a contract. The Contract Act, 1872 provides that where a person who is in a position to dominate the will of another, enters into a contract with him, and the transaction appears, on the face of it or on evidence adduced, to be unconscionable, the burden of proving that such contract was not induced by undue influence shall lie upon the person in a position to

dominate the will of the other. Consequently, in cases of dispute over e contracts the entity carrying out the e-commerce will have the onus to establish that there was no undue influence. Further, the Act also provides that the consideration or object of any agreement is unlawful when it is forbidden by law, or is of such a nature that if permitted, it would defeat the provisions of any law; or is fraudulent, or involves or implies injury to the person or property of another, or the Court regards it as immoral or opposed to public policy. Thus, the entity is also required to keep these prerequisites in mind while entering into an E-transaction[27].

Example :

A consumer visits a bookstore and inquires about the availability of an out-of-stock book. Bookstore employee downloads a digital copy of the book and prints it along with cover. It is not an ecommerce retail transaction since agreement to purchase did not occur over an electronic network. However, the right to access the digital archived copy is an e-commerce service transaction.

A. Some barriers across at the time of jurisdiction of issues related to above they are as following-

B. In the cyberspace, there is no geographical boundary. It establishes immediate long-distance communications with anyone who can have access to any website.

C. No judicial body exists to deal with legal commercial problems arising between citizens of different countries. The court while considering the scope of jurisdiction in International transaction,

D. Bangladesh, all cyber law is governed by the ICT Act. However, ICT Act does not deal with some major legal issues including the issue of jurisdiction. It is well-established law in Bangladesh that where more than one court has jurisdiction in a certain matter, an agreement

27. *E-transaction* hence means a business process where money is transferred electronically from one place into another. It could be through internet

between the parties to confer jurisdiction only on one to the exclusion of the other(s) is valid. In case there is no agreement, the respective court considers the balance of convenience and interests of justice while deciding for the forum.

E. Cyber Crime -Cyber crime is a crime committed over the Internet. It could be against the government, property and against any person in various forms. Nowadays, the law enforcement agencies are facing difficulties in dealing with cyber crime. In Bangladesh, Information Communication and Technology Act, 2006 is the legislation that deals with issue related to cyber crime. Today Cyber crime is a bigger threat to Bangladesh in comparison to physical crime. In a survey Conducted by National crime records Bureau, Ministry of Home Affairs shows that that cyber crime is increasing everyday in various forms.

F. Contractual Difficulties -Recently, Bangladesh has emerged as a major player in the computer software and resources sector. Data shows that Bangladesh will have the largest number of internet-users in Asia in near future. In all e-commerce, the validity and the formation of contract is very essential. The ICA deals with some contractual aspects in E-commerce. However, several practical problems arise when form an electronic contract.

11. Basic forms of E-Contract

Generally the basic forms of "E-Contracts" are mentioned following—

a. The Click-wrap or Web-wrap Agreements.

b. The Shrink-wrap Agreements.

c. The Electronic Data Interchange or (EDI).

11.1. Click-wrap or Web-wrap Agreements :

These are the agreements which generally come across while surfing internet such as "I AGREE" to the terms or "I DISAGREE"

to the above conditions. Now let see the peculiarities of these contracts and the specific industries that put it to use. First and foremost are the Click-wrap agreements. Click-wrap agreements are those whereby a party after going through the terms and conditions provided in the website or program has to typically indicate his assent to the same, by way of clicking on an "I Agree" icon or decline the same by clicking "I Disagree". These types of contracts are extensively used on the Internet, whether it be granting of a permission to access a site or downloading of software or selling something by way of a website. The case of web-click or click-wrap contracts is different as such contracts are formed instantaneously : "The main difference between click-wrap contracts and e-mail is that communications between web clients and servers, unlike e-mails is instantaneous. The best way to imagine the transfer of data between computers is to treat it as a telephone conversation, just one between computers rather than individuals. If either party goes offline at any point, the other will be aware of the change in status. This is because all communications between clients and servers have an inbuilt self-checking mechanism called a check sum."

11.2. The Shrink-wrap Agreements :

These are the agreements generally contains the CD Rom of software. The terms and conditions are printed on the cover of CD Rom. Sometimes additional terms are imposed when in such licenses appear on the screen when the CD is downloaded to the computer. The user has right to return if the new terms and conditions are not to his liking. The validity of the Shrink-wrap agreements first came up for consideration in the famous case of *Pro Cd, Inc v. Zeidenburg*[28] where it was held "that the very fact that purchaser after reading the

---

28. ***ProCD, Inc. v. Zeidenberg***, 86 F.3d 1447 (7th Cir. 1996), is a United States contract case involving a "shrink wrap license". One issue presented to the court was whether a shrink wrap license was valid and enforceable. Judge Easterbrook wrote the opinion for the court and found such a license was valid and enforceable. The Seventh Circuit's decision overturned a lower court decision.

terms of the license featured outside the wrap license opens the cover coupled with the fact that he accepts the whole terms of the license that appears on the screen by a key stroke, constitutes.

11.3. Electronic Data Interchange or (EDI) :

These contracts used in trade transactions which enables the transfer of data from one computer to another in such a way that each transaction in the trading cycle (for example, commencing from the receipt of an order from an overseas buyer, through the preparation and lodgment of export and other official documents, leading eventually to the shipment of the goods) can be processed with virtually no paperwork. Here unlike the other two there is exchange of information and completion of contracts between two computers and not an individual and a computer.

12. Conclusion

It is t pertinent to mention that the Internet as with all path-breaking technological developments gives us all the opportunity to act as a global community, advertise and operate across all frontiers, over borders and beyond the control of any national government, but it also created serious problems, challenges for the legal world in all aspects of law due to its borderless nature. Bangladesh need to promote and facilitate the fair use of cyber space among general masses, to educate civil society groups about the legal constitutional issues, to assure citizens regarding their concern on privacy, personal liberties, to make citizens aware of various kinds of commonly committed cyber offences such as Fraud[29], Identity Theft[30], Hacking[31], Phishing[32] etc. and freedoms and also there is an

---

29. Act or course of deception, an intentional concealment, omission, or perversion of truth.
30. the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit
31. *Hacking* is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

immediate requirement of skilled investigators and trained judges for fair and effective dispute resolution. Bangladesh also needs to identify the possible areas of conflict and operational problems, to address various questions; issues' relating to e-contract and the most appropriate way to start is the creation of a comprehensive legislation which should address broad area of cyberspace taking into consideration, institutional and individual requirements.

The e-contracts have their own merits and demerits. On the one hand they reduce costs, saves time, fasten customer response and improve service quality by reducing paper work, thus increasing automation. With this, E-commerce is expected to improve the productivity and competitiveness of participating businesses by providing unprecedented access to an on-line global market place with millions of customers and thousands of products and services. On the other hand, since in electronic contract, the proposal focuses not on humans who make decisions on specific transactions, but on how risk should be structured in an automated environment. Therefore the object is to create default rules for attributing a message to a party so as to avoid any fraud and discrepancy in the contract.

At present, with the increase in number of internet user, e-contract is organised to grow further. The growing trend of internet banking and credit or debit cards along with the rise in the number of educated and computer literate persons will further support this growth. The need of the hour is law which covers all the aspects of e-contract extending from payment mechanism and maintaining minimum standards in the delivery of services. Such legislation will help to restraint the growth of websites which rise within a few days and then stop functioning in the absence of suitable funds for sustenance. As all business through e-contract sites is ended through the internet without any direct physical interfaces, the main basis

---

32. *Phishing* is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

connections is the trust of the customers which should be engaged at any cost. A law in this field will detect the criminals who have used the internet as a source for making quick money. This will also act a defence for the genuine e-contract websites and help in further growing of business. There is also a need for the creation of an authority in the consumer court to look into the grievances arising out of e-contract transactions. Such an authority should have experts in area such as payment security. This will embolden speedy redressal of disputes and promote e-contract transactions. E-contract which is a developing segment in the commercial arenas scheduled to grow and it is the accountability of the prevailing players to ensure that growth is not hindered by their acts and policies.

CHAPTER SEVEN

E-learning

1. Meaning of E-Learning

E-learning is the transmission of skills and information via a network. E-learning is a method of learning that involves the use of electronic applications and procedures. Web-based learning, computer-based learning, virtual classrooms, and digital collaboration are all examples of electronic applications in e-learning. The internet, audio or video tape, satellite TV, and CD-ROM are all used to provide learning materials. E-learning allows you to study at your own pace.

The term 'E-Learning' means 'electronic Learning' that encompasses all forms of technology enhanced learning. E-Learning is the use of technology to enable people to learn anytime and anywhere. E-Learning can include training, the delivery of just-in-time information and guidance from experts. These services are delivered, enabled or mediated by ICT[1] for the purposes of delivering education.

E-Learning is a catch-all term that covers a wide range of instructional material that can be delivered on a CD-ROM or DVD, over a LAN[2], or on the Internet. It includes CBT[3], WBT[4], EPSS[5], distance or online learning and online tutorials. The major advantage to students is its easy access.

2. The history of E-Learning

The term "e-learning" has only been around since 1999, when it was coined at a CBT systems lecture. Other terms, such as "online

---

1. Information & Communication Technology Act, 2006
2. Local area network
3. Computer-Based Training
4. Web-Based Training
5. Electronic Performance Support Systems

learning" and "virtual learning," sprung developed in quest of a more precise definition. The concepts of e-learning, on the other hand, have been extensively recorded throughout history, and there is even evidence that early versions of e-learning existed as early as the nineteenth century.

Distance courses were available even before the internet was introduced to give students with instruction on certain topics or abilities. Isaac Pitman used letters to teach his students shorthand in the 1840s. This kind of symbolic writing was popular among secretaries, journalists, and other people who had to take a lot of notes or write a lot. Pitman, a certified instructor, received completed assignments via mail and then gave his pupils additional work to complete using the same method.

The first testing machine was developed in 1924. Students were able to test themselves using this gadget. Then, in 1954, Harvard Professor BF Skinner developed the "teaching machine," which allowed schools to provide pupils pre-programmed lessons. However, the first computer-based training program was not presented to the world until 1960. PLATO-Programmed Logic for Automated Teaching Operations was the name of this computer-based training software (or CBT program). It was created for University of Illinois students, but it has since been adopted by institutions across the region.

The earliest online learning systems were primarily designed to provide students with knowledge, but as the 1970s progressed, online learning began to become more participatory. The Open University in the United Kingdom was eager to take advantage of e-learning. Their educational system has traditionally been mainly centered on remote learning. Course materials and contact with instructors were formerly provided by mail. The Open University started to provide a broader variety of interactive educational experiences as well as quicker communication with students through email and other means with the advent of the internet.

3. Online learning today

E-learning technologies and delivery techniques grew in popularity when the computer and internet were introduced in the late twentieth century. Individuals were able to have computers in their homes for the first time in the 1980s, making it simpler for them to learn about certain topics and acquire specific skill sets. People had access to a plethora of online knowledge and e-learning possibilities in the next decade, and virtual learning environments started to flourish.

By the early 1990s, many colleges had been established that exclusively offered online courses, using the internet to provide education to individuals who previously would not have been able to attend a college owing to geographic or temporal limitations. Technological advances also assisted educational institutions in lowering the expenses of remote learning, which was passed on to students, allowing education to reach a larger audience.

Businesses started utilizing e-learning to educate their workers in the early 2000s. New and seasoned employees both now have the chance to develop their skill sets and improve their industry expertise. Individuals were given access to programs at home that allowed them to obtain online degrees and improve their life by expanding their knowledge.

4. Merits of E-Learning

E-learning offers many benefits that more traditional training options, such as facilitated sessions or lectures, don't provide. For example, e-learning...

1. **Can be either an asynchronous or synchronous activity :** Traditionally, e-learning has been asynchronous, which means there is no predetermined time for the learning to take place. Everyone can go at their own pace, and take their time to learn what they need to know, when they need to know it. However, more synchronous e-learning is now being offered through web conferencing and chat options. The great thing about e-learning is it gives you the option to do one, or both.

2. **Has a global reach :** E-learning can simply be placed online and easily accessed by people around the world. There is no need for expensive travel or meetings across multiple time zones.
3. **Spans multiple devices/mobile :** Online courses can work on computers as well as on mobile devices, such as smartphones and tablets. This means e-learning courses can literally be in the hands of the people who need them, at all times.
4. **Is just-in-time/needs-based :** E-learning authoring software is so easy to use that anyone can create, publish, and share a course within a few hours, allowing you to provide people with resources and training they can access right when they need it.
5. **More efficient :** With e-learning, you can develop a course that can be distributed electronically to thousands instead of having to organize in-person training sessions whenever people need to be brought up to speed.
6. **Reduces costs :** All of the abovementioned factors result in a cost savings for organizations that use e-learning courses to replace some of their traditional instructor-led training.
7. **Allows for consistent quality and content :** When develop an e-learning course, it can deliver the same message to all learners consistently. In classroom training, the message, equipment, and other conditions can vary widely from one session to the next, which can affect the outcome of the course.

5. Methods of Sharing E-Learning

Once created an e-learning course, you need to distribute it to learners. There are many ways to do this, and—like everything else related to e-learning—those ways are constantly evolving and improving. There are two ways to share content : informal distribution and formal distribution.

5.1. Informal Distribution

Informal distribution of e-learning content typically means users are trusted to view the e-learning course, and their participation isn't tracked or scored. One way to informally share an e-learning course is to put it on a web server, then send participants the link and have them view the course. You don't really have a systematic way of knowing whether learners have completed the course, but sometimes that's not necessary.

5.2. Formal Distribution

Sharing an e-learning course formally means there's a need to track and record learner results. Most organizations that have a need for formal distribution of e-learning have specific systems and standards in place for this.

Tracking is usually done in what is called a Learning Management System (LMS). Certain standards are in place to report the information to the LMS, including AICC, SCORM, and, more recently, Tin Can.

6. The benefits and drawbacks of online learning

Important benefits are outlined below :

6.1. No Boundaries, No Restrictions

Along with locational restrictions, time is one of the issues that learners and teachers both have to face in learning. In the case of face-to-face learning, the location limits attendance to a group of learners who have the ability to participate in the area, and in the case of time, it limits the crowd to those who can attend at a specific time. E-learning, on the other hand, facilitates learning without having to organize when and where everyone who is interested in a course can be present.

6.2. More Interactive

Designing a course in a way that makes it interactive and fun through the use of multimedia or the more recently developed methods of gamification enhances not only your engagement factor but also the relative lifetime of the course material in question.

6.3. Cost Effective

This is directed to both learners and teachers, but there is a good chance that whatever your role you had to pay exorbitant amounts of money at some point to acquire updated versions of textbooks for school or college. While textbooks often become obsolete after a certain period of time, the need to constantly acquire new editions is not present in e-learning.

6.4. Corporate Necessity

As companies and organizations adopt technologies to improve the efficiency of day-to-day operations, the use of the internet becomes a necessity. As multinational corporations expand across the globe, the chances of working with people from other countries increases, and training all those parties together is an issue that e-learning successfully addresses. And that's a great advantage of online learning.

6.5. Concerns that arise with e-learning

Even given all the benefits of e-learning, one cannot deny there are some drawbacks. A good example of a disadvantage of online learning is that practical skills are somewhat harder to pick up from online resources. For example, although building a wooden table is something you can easily share information about, record videos of and explain, the practical experience is essential. Pottery and car engineering are examples of skills that require hands-on experience.

6.6. Isolation

Though e-learning offers ease, flexibility and the ability to remotely access a classroom in the student's own time, learners may feel a sense of isolation. This is because learning online is a solo act for the most part, which may give the learner the feeling that they are acting completely alone. As technology progresses and e-learning benefits from the advancements being made, learners can now engage more actively with professors or other students using tools such as video conferencing, social media, and discussion forums amongst others.

6.7. Health-Related Concerns

E-learning requires the use of a computer and other such devices; this means that eyestrain, bad posture and other physical problems may affect the learner. When running an online course it's a good practice to send out guidelines about correct sitting posture, desk height, and recommendations for regular breaks.

7. Important Terminology of E-Learning :

Here are a few important terms to understand related to the distribution of e-learning :

a. **LMS :** LMS stands for Learning Management System and refers to software used to administer, track, report, and document the delivery of e-learning courses.

b. **SCORM :** The Shareable Content Object Reference Model is a collection of specifications and standards for e-learning, which allows e-learning course to communicate with your LMS.

c. **Tin Can API (or xAPI) :** Tin Can API (Application Programming Interface) is a new specification for e-learning that collects data about a person's learning experiences across various devices and platforms.

d. **AICC :** The Aviation Industry Computer-Based Training Committee is a set of specifications designed so learning technology vendors could spread their development costs across multiple markets. While some LMSs still use this standard, most experts agree that it's fairly outdated.

CHAPTER EIGHT
Prevention of Cyber Crimes

1. Introduction :

In recent years, computer crime, also known as cyber crime, has grown in severity and regularity, and as a result, it has become a significant source of worry for businesses, colleges, and organizations. Governments, police departments, and intelligence agencies all around the globe have begun to respond against cybercrime. This chapter offers an introduction of cyber crime and analyzes knowledge of the issue among various respondents in Bangladesh, as well as highlighting the severity of the problem and the urgent need to mitigate its global effect.

Cyber crime is still a low priority in Bangladesh. Though computers are becoming common house hold items and the numbers of internet users have already crossed thirty millions, very few computer related offences are reported to the police. In Bangladesh there is no Computer Emergency Response Team (CERT),[1] no cyber police or virtual police to handle the incidents such as computer abuses, hack attempts and other information security breaches. Bangladesh has enacted the Information and Communication Technology ACT of 2006[2] with a maximum punishment of 14 years of imprisonment or maximum fine of 10 million taka[3] or with both for a cyber crime. Still the legislation seems not to be sufficient to effectively fight cyber crimes in the country.

---

1. Computer Emergency Response Team' may be called CERT throughout the study.
2. Act no 39 of 2006.
3. Bangladeshi currency.

The present Government is expected to invest millions of taka to materialize its promise to build a digital Bangladesh. This is why the issue of prevention of cyber crime must get due priority and a considerable portion of budget should be allocated to ensure the issue. This chapter finds the policy of prevention of cyber crimes in Bangladesh and also provides some sort of recommendations.

2. Effects of Cyber Crime

Criminals make use of technology in a variety of ways. Scammers and other criminals benefit greatly from the Internet because it enables them to do their business while remaining anonymous online. Cybercrime has an impact on society in a variety of ways, both online and offline.

2. 1. Economic Impacts

Because cybercrime is designed to harm the image of a person, a commercial company, or a government agency, it has a significant economic impact, such as when a financial institution's system, such as a bank, is hacked. In every transaction, banks and their customers must operate in good faith. Banks must maintain their good faith by not leaking a client's information, since this may lead to a cold war. When a cyber-criminal successfully hacks into a bank's system, the bank's good faith is jeopardized, since the criminal may steal a client's money or publish the client's personal information on a website, eroding the customer's confidence. This tarnishes a bank's reputation, since the customer may be ready to seek out better opportunities.[4]

2. 2. Social Impacts

Trying to overcome a cyber attack for a developing country may not a good experience, as trying to mend the damage might cost

---

4. Nadia Khadam, Insight to Cybercrime, available at http :// www. hanyang.ac.kr/ home_news/H5EAFA/0002/101/2012/29-3.pdf,(accessed 4 February 2016).

millions of dollars which may not be readily available. Due to cyber attacks, the citizens of developed or developing countries start avoiding the advent of technology as they feel insecure. This may destroy the concept of globalization as people might not want to be a part of social networking.[5]

2. 3. Political Impacts

Cyber crime has a big impact on the political world, particularly when governmental computer networks are targeted and attacked. This decreases the ability of international organizations investing resources in developing countries.[6] When this happens it increases white collar criminal activities and funding of anti-government regimes in order to the Government, which will definitely affect the political scenes in a country.

3. Survey

Due to the exploratory nature of the task, survey questions provide a basis for the research in order to find the awareness of cyber crime among the respondents as well as to find out what type of cyber crimes are occurring these days in Bangladesh and what should be done to prevent Cyber Crime.

3.1. Sample and Respondents

The primary target respondents are working professionals who are aware of the various computer crimes and security issues within their organizations. Typically, they are senior managers, IT[7] administrators and IT security consultants. Simple random sampling is the primary sampling method used when selecting the sample for survey.

---

5. Ibid.
6. '*International Journal of Engineering Sciences and Emerging Technologies*,' vol.6, no.2, 2013, pp. 142-153.
7. The term `information technology' may be meant by IT throughout the study.

3. 2. Results and Findings

In conducting the research, the researcher uses SPSS[8] 13.0 software program and takes the hypothesis that there is no association between respondents' occupation and the level of cyber crime awareness.

3.2.1 Lack of Awareness (Table : 1)

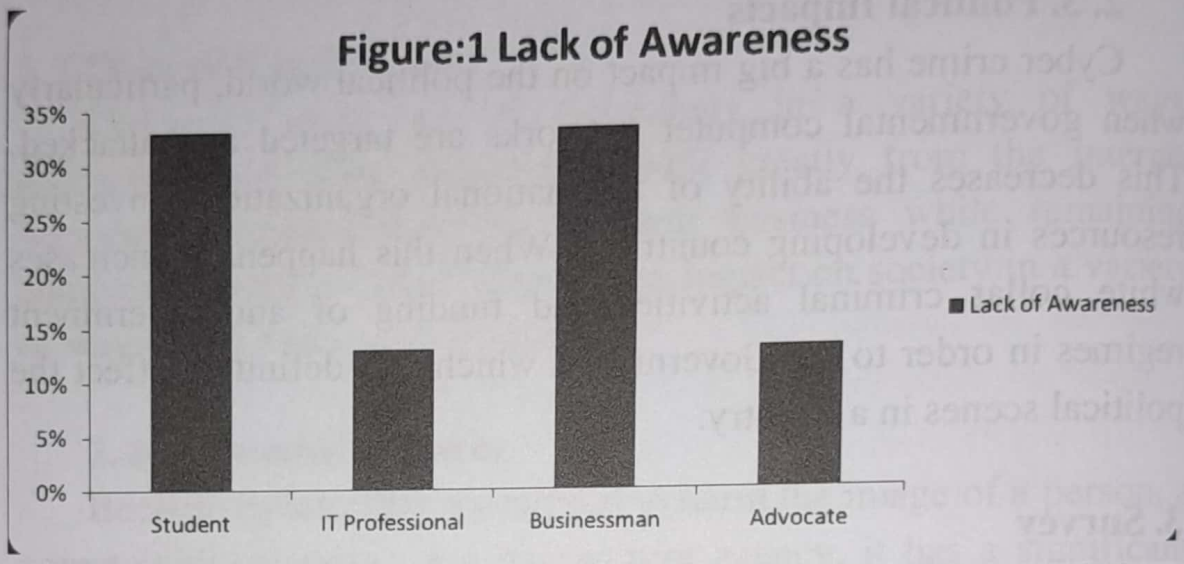
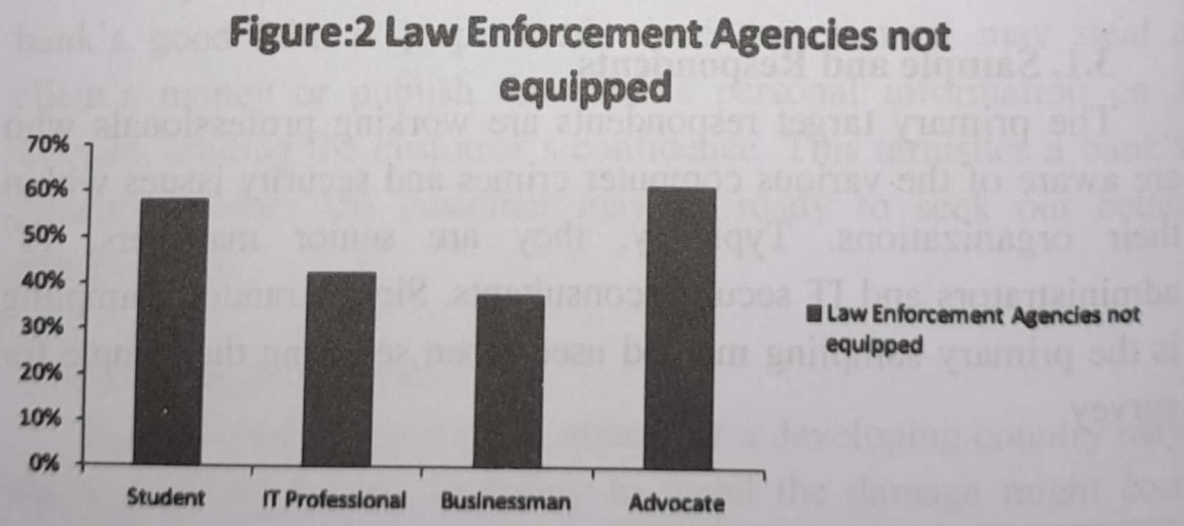


Table 1 shows that among the respondents 33% students, 13% IT professionals, 33% businessmen and 13% advocates think that major drawbacks, which prevent cyber crimes from being solved in Bangladesh, is lack of awareness among the people.

3.2.2. Law Enforcement Agencies not equipped (Table : 2)



8. SPSS is a widely used program for statistical analysis in social science. It is also used by market researchers, health researchers, survey companies, government, education researchers, marketing organizations, data miners and others.

Table 2 shows that among the respondents 58% students, 42% IT professionals, 37% businessmen and 61% advocates are of the view that law enforcement agencies are not fully equipped with handling cyber-criminal activities.

3.2.3. All Factors (Table : 3)

Figure 3: All Factors

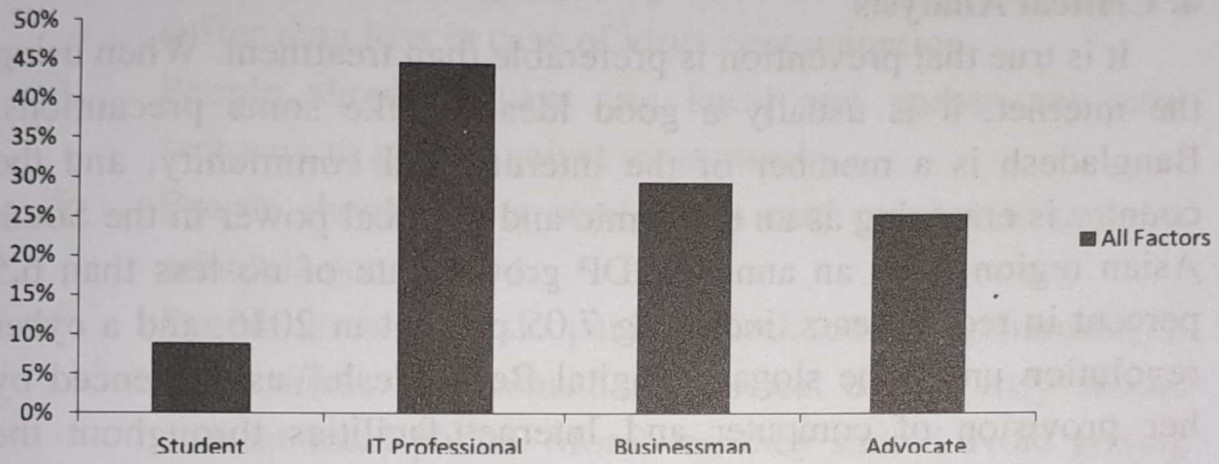


Table 3 shows that among the respondents 9% students, 45% IT professionals, 30% businessmen and 26% advocates feel that all the factors are responsible for preventing cyber crimes to be solved in Bangladesh.

3.2.4. Spreading Cyber Crime (Table : 4)

Figure:4 Spreading Cyber Crime

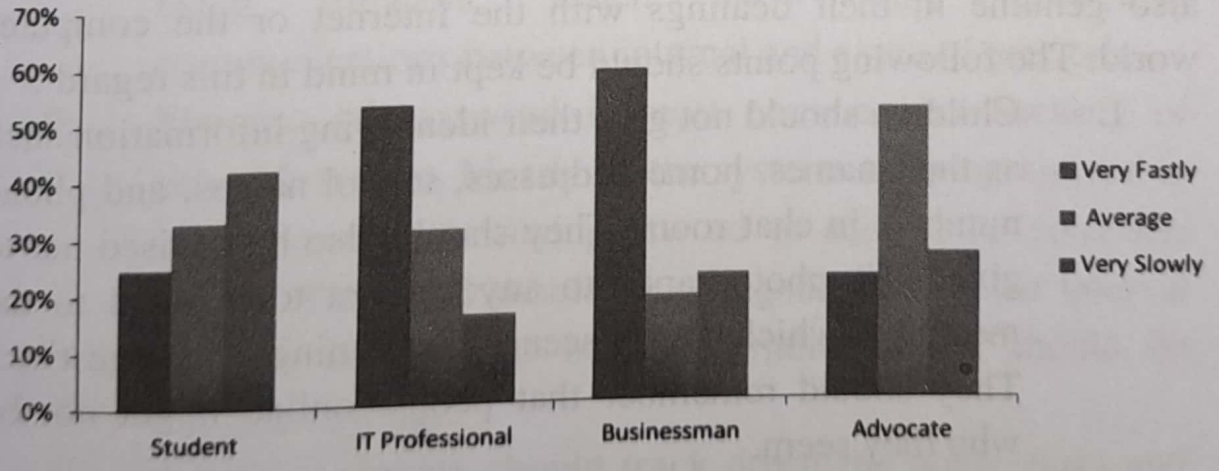


Table 4 shows that out of the respondents, on the issue of spreading the disease of cyber crime these days, 25% students, 53%

IT professionals, 59% businessmen and 22% advocates feel that it is spreading very fast; and 33% students, 31% IT professionals, 18.5% businessmen and 52% advocates are of the opinion that it is spreading at an average; whereas 42% students,16% IT professionals, 22.5% businessmen and 26% advocates believe that it is spreading very slow.

4. Critical Analysis

It is true that prevention is preferable than treatment. When using the internet, it is usually a good idea to take some precautions. Bangladesh is a member of the international community, and the country is emerging as an economic and political power in the South Asian region, with an annual GDP growth rate of no less than 6.5 percent in recent years, including 7.05 percent in 2016, and a cyber revolution under the slogan "Digital Bangladesh," as evidenced by her provision of computer and Internet facilities throughout the country. It has the potential to damage not only the Internet environment, but also the country's economic situation and growth, as shown by the recent Reserve Hacking of 80 billion US dollars at the Bangladesh Bank, the country's central bank. All of the nation's economic, social, and political environments, as mentioned above, may become susceptible as a result of cyber criminal actions that occur inside or outside the country. As a result, it is past time for the people of the nation to become not only conscious of the problem but also genuine in their dealings with the Internet or the computer world. The following points should be kept in mind in this regard :

1. Children should not give their identifying information such as their names, home addresses, school names, and phone numbers in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive.[9] They should remember that people online might not be who they seem.

---

9. https ://www.privacyrights.org/content/childrens-safetyinternet(accessed 1 July2015).

2. Parents should use content filtering software on their computers so that their child is protected from pornography, gambling, drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3. People should keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4. People should always use latest and update anti-virus software to guard against virus attacks.
5. People should never send credit card number to any site which is not secured.
6. People should not do panic if find something harmful. If there arises any immediate physical danger they should contact local police. Moreover, they should avoid getting into huge arguments online during chat and discussions with other users, and be careful about personal information about themselves online.
7. People should be cautious on meeting online introduced person. They should try to keep record of all communication for evidence and not edit it any way.
8. Big organizations should implement access control system using firewalls, which allow only authorized communications between internal and external network.
9. The use of password is most common for security of network system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.
10. System managers should track down the holes, bugs and weaknesses in the network before the intruders do.

5. Practices Recommended for Cyber Crime Prevention in Bangladesh

Cyber attacks could emerge as a major threat to the digital transformation of Bangladesh given the poor knowledge and lack of government initiatives to counter the growing problem, according to the study. Therefore it is always better to take certain precaution while operating the net.

1. **Firewalls**[10] **:** These are programs that protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom the user permits.
2. **Frequent password changing :** With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.
3. **Safe surfing :** Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, and visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimize the risk.
4. **Frequent virus checks** : One should frequently check ones computer for viruses and worms. Also any external medium such as floppy disks and CD[11] ROMS[12] should always be virus checked before running.

---

10. A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
11. A compact disc [sometimes spelled *disk*] (CD) is a small, portable, round medium made of moulded polymer (close in size to the floppy disk) for electronically recording, storing, and playing back audio, video, text, and other information in digital form.
12. Pronounced *rahm*, acronym for *read-only memory*, computer memory on which data has been pre recorded. Once data has been written onto a ROM chip, it cannot be removed and can only be read.

5. **Email filters :** These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
6. **Online photography :** Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
7. **Undergo :** Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
8. **Credit Card security :** To guard against frauds one should never send credit card number to any site that is not secured.
9. **Depravation in children :** Always keep a watch on the sites that children are accessing for the purpose of preventing any kind of harassment or depravation in children.
10. **Secure the Program :** It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
11. **Watching Traffic :** Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
12. **Protecting internal network :** Web servers running public sites must be physically separate and protected from internal corporate network.
13. **Backup :** Make Backups of Important Files and Folders to protect important files and records on computer if one's computer malfunctions or is destroyed by a successful attacker.
14. **Off internet :** Disconnect from internet when not in use.

Some other advises to be addressed while using the Internet or computers :

1. Habitually download security protection update patches & keep your browser and operating system up to date.

2. Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
3. Disable file sharing on computers.
4. Turn off the network during extended periods of non-use, etc.
5. Check online account frequently and make sure all listed transactions are valid. Use a variety of passwords, not the same for all the accounts.
6. Never respond to text messages from someone unknown.
7. Avoid posting cell phone number online.
8. Open email attachment carefully.

6. Policies Recommended for Prevention of Cyber Crime in Bangladesh

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bringing into practical part so that the practices become easier to implement. Policies recommended are as follows :

1. Integrated policies are required to ensure the effective benefits from the information system. The basic challenge and issue in the development of a cyber society is the lack of financial and trained human resources.
2. A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secured and free from cyber crime and within the reach of a common man.
3. Promotion of research & development in ICT[13] area and also in Human Resource is to be a core part of the system.

---

13. ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing : radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

4. Up-to-date, common, and mutually supporting cyber laws should be there to fight with cyber crimes and protection of intellectual property rights towards the creation of cyber-crime free information society.
5. Adoption of ICT standards, regulation, and quality assurance is a necessity to foster high quality of services and productions that keep competition in place for the benefits of the communities within each country.
6. High levels of awareness in each part of the society should be there in regard to information security and cyber crimes and increased exchange of information on information security and cyber crime at the regional and national levels should be there.
7. Effective mechanisms should be there for the detection and prevention of cyber crimes and for improving protection against, detection of, and responses to, cyber crimes, at the lower level itself.
8. Conducting national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and private sector using different media is also a must.
9. The government should educate and involve the media professionals, and then encourage them to increase public awareness.
10. People should engage large private sector corporations and industry associations in the sponsorship of awareness programs.
11. Stress should be laid on less developed countries on effective systems for protection against, detection of and responses to, cyber crime.
12. People should promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.
13. Law enforcement personnel must be trained and equipped in addressing high-tech crimes. Legal systems should

permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

14. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
15. People should use established network of knowledgeable personnel to ensure a timely and effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis.
16. The government should welcome outsourcing initiatives to prepare a galaxy of virtual police officers and establish few cyber police stations across the country as soon as possible. These cyber crime fighters should be given specialized training home and abroad.
17. Awareness raising, education, and technical support to prevent e-crime[14] is essential, but without discouraging the development of e-commerce.

7. Minimizing the Risk of Becoming a Cyber Crime Victim

As widespread as cybercrime appears to be, it would be easy to conclude there is little anyone can do to avoid becoming a victim. However, the prevalence of cybercrime does not mean that victimization is inevitable or that people should avoid using the Internet. Users can make themselves aware of the vulnerabilities its use creates and can take steps to reduce their risks.

1. Use strong passwords : Use separate ID[15]/password combinations for different accounts, and avoid writing them down. Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis.[16]

---

14. E-crime is any form of anti-social behaviour over the internet or via electronic devices. It is an attack or abuse, using technology, which is intended to cause another person harm, distress or personal loss.
15. Own password for access different digital account.
16. The Office of Angel Cruz, Chief Information Security Officer, State of Texas September 2012 , Volume 6, Issue 8

2. To secure computer : Firewalls are the first line of cyber defence; they block connections from suspicious traffic and keep out some types of viruses and hackers.

3. Use anti-virus/malware software : Prevent viruses from infecting computer by installing and regularly updating anti-virus software.

4. Block spyware attacks : Prevent spyware from infiltrating computer by installing and updating anti-spyware software.

5. Secure the mobile device : Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources only. Do not store unnecessary or sensitive information on mobile device. Most importantly, keep the device physically secured; millions of mobile devices are lost each year. In case of loss of dévice, report it immediately to carrier and/or organization. Some devices allow remote data erasing. Always protect mobile device password.[17]

6. Install the latest operating system updates : Keep applications and operating system, e.g., Windows, Mac, Linux,[18] current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

7. Protect the data : Use encryption for most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of important data.

8. Secure the wireless network : Wi-Fi[19] (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid conducting sensitive transactions on these networks.

9. Protect e-identity : Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secured, especially when making online purchases, or ensure that enabled privacy settings, e.g., when accessing/using social networking sites,

---

17. Ibid.
18. Applications of computer operating system may be called Windows, Mac, Linux throughout the study.
19. WiFi is a technology that uses radio waves to provide network connectivity.

such as Facebook, Twitter, YouTube, etc. Once something is posted on the Internet it may be there forever.

10. Avoid being scammed : Never reply to emails that ask to verify your information or confirm your user ID or password. Don't click on a link or file of an unknown origin. Check the source of the message; when in doubt verify the source.

8. Recommendations

The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their "attack surface" and mitigate the risks. For this purpose the following recommendations may be proposed.

8.1 Education on Cyber Crimes :

Education is the most important strategy that can be used in combating crimes in the cyberspace. People can be educated in workshops and seminars specially planned by organizations taking into account cyber safety. It is recommended that this should be done on a regular basis as new employees are always recruited. In doing so employees or system users may learn how to keep personal and organization information safe, then the cyber-criminals will flee. The study shows that most of the cyber-criminals of Bangladesh are youths, students of tertiary institutions, or they have graduated from tertiary institutions. It is recommended that tertiary institutes should introduce studies on cyber crimes, and cyber management and its prevention as part of their course curriculum. In doing so the present social changes happening in the country are to be addressed.

8.2. Creating Cyber Employment :

The Government should act swiftly on domestic cyber crime legislations and enact a comprehensive law on cyber crimes. In order for the law to be effective and efficient the Government should

empower graduates by providing employment or funds to be able to employee themselves with their ideas on cyber-crimes.[20]

8.3. Providing Training :

The Bangladesh Government should also make provisions for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals, whatever intelligent and cunning they may be.

8.4. Cooperation to Government :

For the government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb cyber crimes, it is recommended that there is a need for them to understand the technology and the individuals who engage in such criminal acts. The findings show that cyber criminals are part and parcel of the society, as such, prevention of cyber crimes requires the cooperation of all the citizens and not of the law enforcement agencies alone.

8.5. Identification of Cyber Criminals :

Everyone should watch and report to law enforcement agencies quickly when they feel someone is being involved in the commission of cyber crimes. This enables the government to bring the cyber criminals to the books of law.

8.6. Ensuring Punishment :

The assets of the cyber criminals should be confiscated by the government and the imposition of longer prison terms should be enacted for cyber criminals in domestic legislation. This may serve as deterrent to those youths who want to indulge in heinous cyber crimes.

8.7. Circulating Current Trends :

Innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICT;

---

20. S.J. Schjolberg, 'An International Criminal Tribunal for Cyberspace : Cybercrime Legal Work Group, Geneva, (2007-2008).

through this they can not only be well informed about the current trends in cyber crimes but also gather knowledge on different forms of the said crimes, and the methods how the cyber criminals carry out their bad activities. Thereby they can devise means of protecting their information from cyber criminals.

8.8. Drawing Consciousness :

Internet users should be conscious of security. In simple words, they must learn how not to provide personal or financial information to others unless there is a legitimate and assumed reason. They should not, for instance, throw out cheques, old credit cards, driving licenses, passports, receipts and other numerous documents containing personal data.

8.9. Awareness of Internet Service Provider :

The internet service providers should not just provide broadband connection to their subscribers, but they should also monitor effectively what the subscribers are doing on the internet. They should provide their customers, especially financial institutions and cyber cafes with well guided security codes and packages in order to protect their information and software from hackers and publishers.

9. Conclusion

People in Bangladesh are becoming more vulnerable to cybercrime. Computers have an impact on every aspect of contemporary life. Cybercrime is an issue that affects everyone. Without a question, the Internet provides thieves with unrivaled possibilities. There's a lot that can be done to guarantee a secure and reliable computer environment. It is critical not just for one's own well-being, but also for Bangladesh's national security. In light of recent technological advancements, it is not simple or feasible to eradicate cybercrime from society once and for all, but it is quite possible to fight and monitor it. The first and most important prerequisite for achieving the goal is for people to be aware about cybercrime and the measures that may be taken to avoid it.

CHAPTER NINE
E-governance

1. Introduction

Information and communication technologies are undergoing a global revolution. The Internet, personal computers, and cell phones are all profoundly altering our lives, influencing how we work, study, and connect. The importance of e-Government is being recognized by governments all around the globe. E-Government may increase efficiency in the delivery of government services, simplify compliance with government laws, promote public involvement and confidence in government, and save money for people, companies, and the government itself provided it is properly planned and executed. As a result, policymakers and managers in nations all over the globe, from the most developed to the least developing, are seeking to implement e-Government.

2. Definition

Different academics have defined governance in various ways. The word government comes from the word "govern," which comes from Old French "governer," or Latin "gubernare," which means "to steer or rule," and the Greek word "kubernan," which means "to steer," and is steeped in controlling, or at least having a large (and possibly invasive) role in citizens' lives.

The main criteria that society puts on its government are often used to define governance. Government is defined by the New Oxford English Dictionary (2001) as "the system by which a state or society is ruled" or "the activity or method of governing or regulating a state, organization, or people." Other popular definitions include "the exercise of political power over the acts or affairs of a political unit, people, or other body, as well as the execution of

specific duties for this unit or body" and "the executive policymaking body of a political unit, community, or other body."

In general, e-Government refers to the use of Information Communications Technology (ICT) by the appropriate government entity to provide information and public services to the public. In basic words, e-Government is the use of technology to improve citizen, business partner, and employee access to and delivery of government services. It is the use of information technology to assist government operations, engage people, and deliver more efficient and transparent public services.

3. Benefits of E-Governance

According to the World Bank (2002) E-Governance has the following benefits;

a. It makes the process of gathering information for individuals and companies easier.

b. It empowers people to gather information regarding any department of government and get involved in the process of decision making.

c. E-Governance strengthens the very fabric of democracy by ensuring greater citizen participation at all levels of governance

d. E-Governance leads to automation of services, ensuring that information regarding every work of public welfare is easily available to all citizens, eliminating corruption.

e. This revolutionizes the way governments function, ensuring much more transparency in the functioning, thereby eliminating corruption.

f. Since the information regarding every activity of government is easily available, it would make every government department responsible as they know that every action of theirs is closely monitored.

g. Proper implementation of e-Governance practices make it possible for people to get their work done online thereby

sparing themselves of unnecessary hassles of traveling to the respective offices.

h. Successful implementation of e-Governance practices offer better delivery of services to citizens, improved interactions with business and industry, citizen empowerment through access to information, better management, greater convenience, revenue growth, cost reductions etc.

Furthermore, the use of e-Government brings governments and people closer together. So much so that contacting a government entity has become very easy in recent years. Citizens' service centers are increasingly placed closer to citizens. An unattended kiosk at a government agency, a service kiosk near to the customer, or the usage of a personal computer in the home or workplace are examples of such centers.

4. Advantages of E-Governance

a. Speed

Communication has become more rapid as a result of technological advancements. Smartphones and the Internet have made it possible to send large amounts of data across the globe in real time.

b. Saving Costs

The expense of purchasing official stationery accounts for a large portion of government spending. Letters and other written documents use a lot of paper. However, replacing them with Smartphones and the internet may save billions of dollars each year in costs.

c. Transparency

The use of e-governance helps make all functions of the business transparent. All Governmental information can be uploaded onto the internet. The citizen's access specifically access whichever information they want, whenever they want it, at the click of a mouse, or the touch of a finger.

However, for this to work the Government has to ensure that all data as to be made public and uploaded to the Government information forums on the internet.

d. Accountability

Transparency directly links to accountability. Once the functions of the government are available, we can hold them accountable for their actions.

5. Disadvantages of E-Governance

a. Loss of Interpersonal Communication

The main disadvantage of e-governance is the loss of interpersonal communication. Interpersonal communication is an aspect of communication that many people consider vital.

b. High Setup Cost and Technical Difficulties

Technology has its disadvantages as well. Specifically, the setup cost is very high and the machines have to be regularly maintained. Often, computers and internet can also break down and put a dent in governmental work and services.

c. Illiteracy

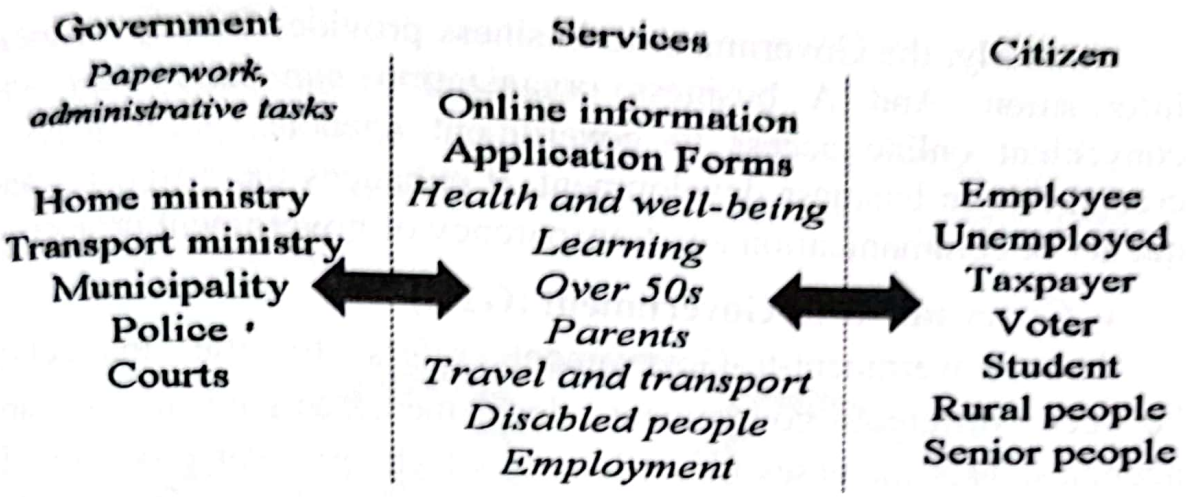
A large number of people in India are illiterate and do not know how to operate computers and smart phones. E-governance is very difficult for them to access and understand.

6. Types of E-Governance

E-Governance is of 5 types depending on the specific types of services.

a. Government-to-Citizen(G2C)

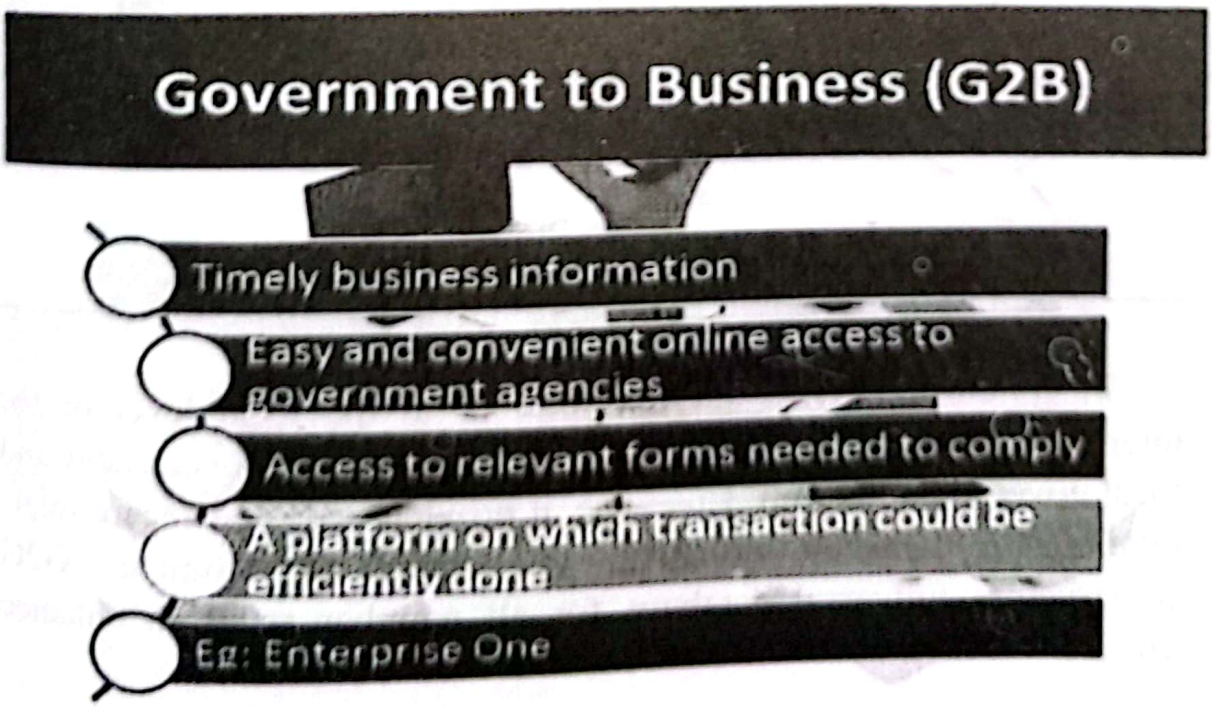
The term "government-to-citizen" refers to government services that are available to ordinary citizens. G2C encompasses the majority of government services. Similarly, the main aim of government-to-citizen communication is to offer services to citizens. It enables regular people to save time and money while doing transactions. Citizens may use the services at any time and from any location.



Furthermore, Many services like license renewals, and paying tax are essential in G2C. Likewise, spending the administrative fee online is also possible due to G2C. The facility of Government-to-Citizen enables the ordinary citizen to overcome time limitation. It also focuses on geographic land barriers.

b. Government-to-business (G2B)

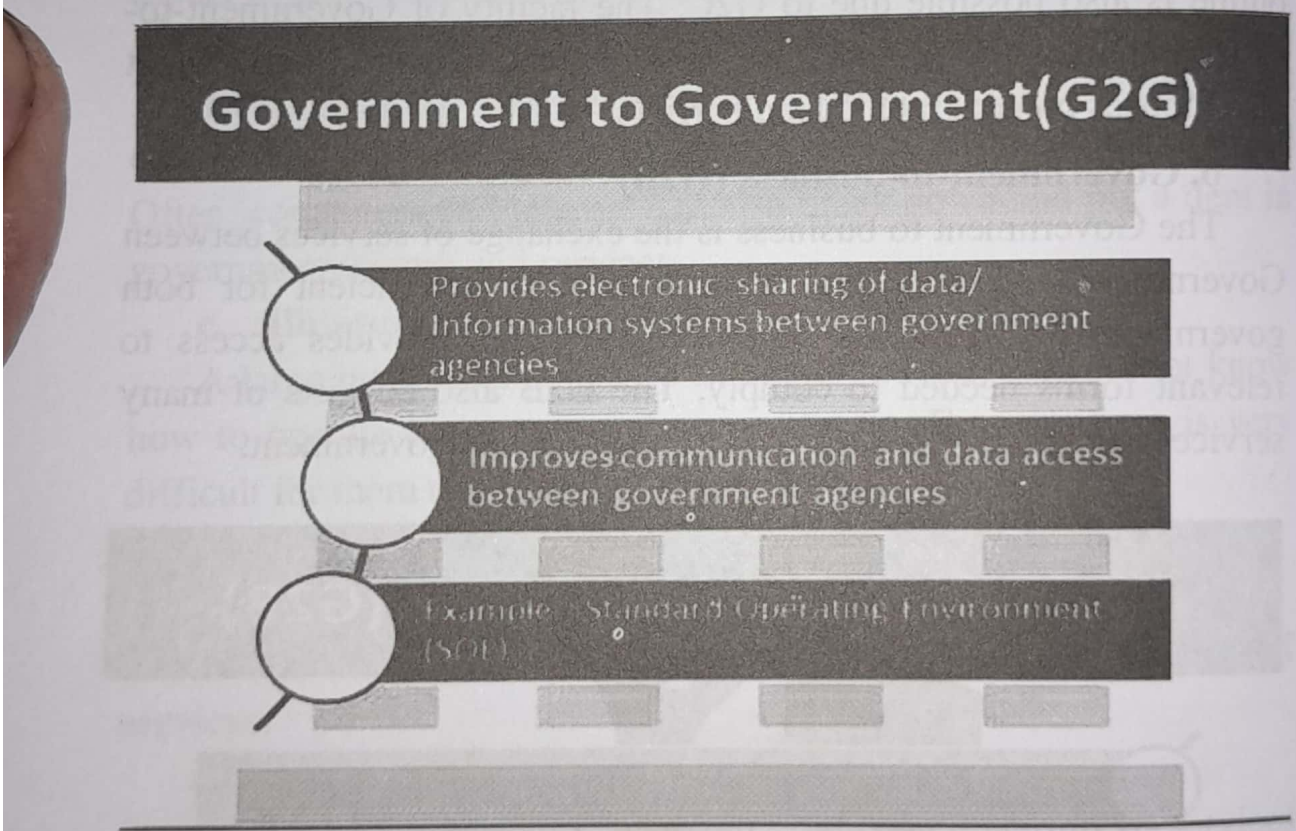
The Government to business is the exchange of services between Government and Business organizations. It is efficient for both government and business organizations. G2B provides access to relevant forms needed to comply. The G2B also consists of many services exchanged between business sectors and government.



Similarly, the Government to business provides Timely business information. And A business organization can have easy and convenient online access to government agencies. G2B plays a crucial role in business development. It enhances the efficiency and quality of communication and transparency of government projects.

c. Government-to-Government (G2G)

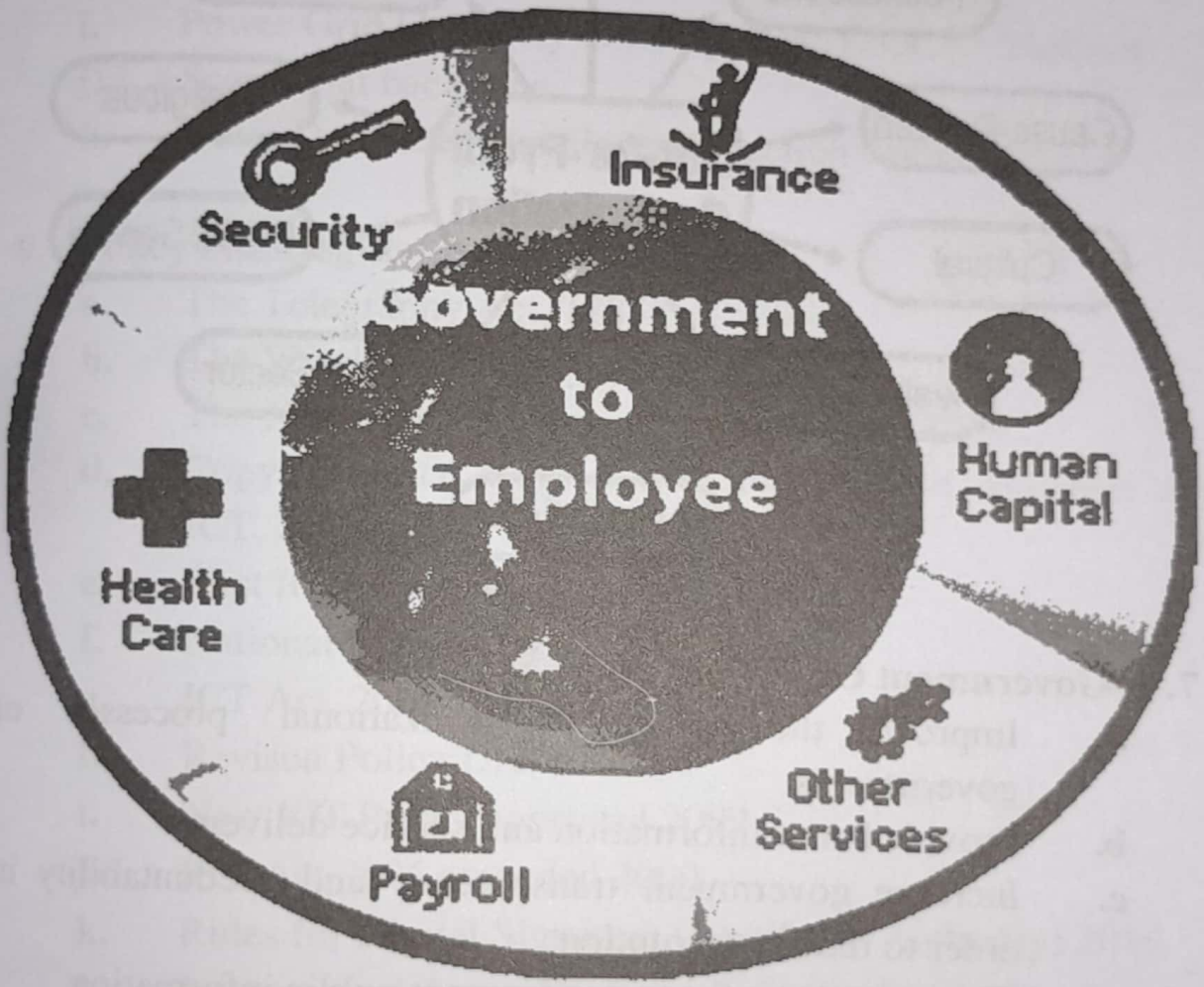
The Government-to-Government refers to the interaction between different government department, organizations, and agencies. This increases the efficiency of government processes. In G2G, government agencies can share the same database using online communication. The government departments can work together. This service can increase international diplomacy and relations.



In conclusion, G2G services can be at the local level or the international level. It can communicate with global government and local government as well. Likewise, it provides safe and secure inter-relationship between domestic or foreign government. G2G constructs a universal database for all member states to enhance service.

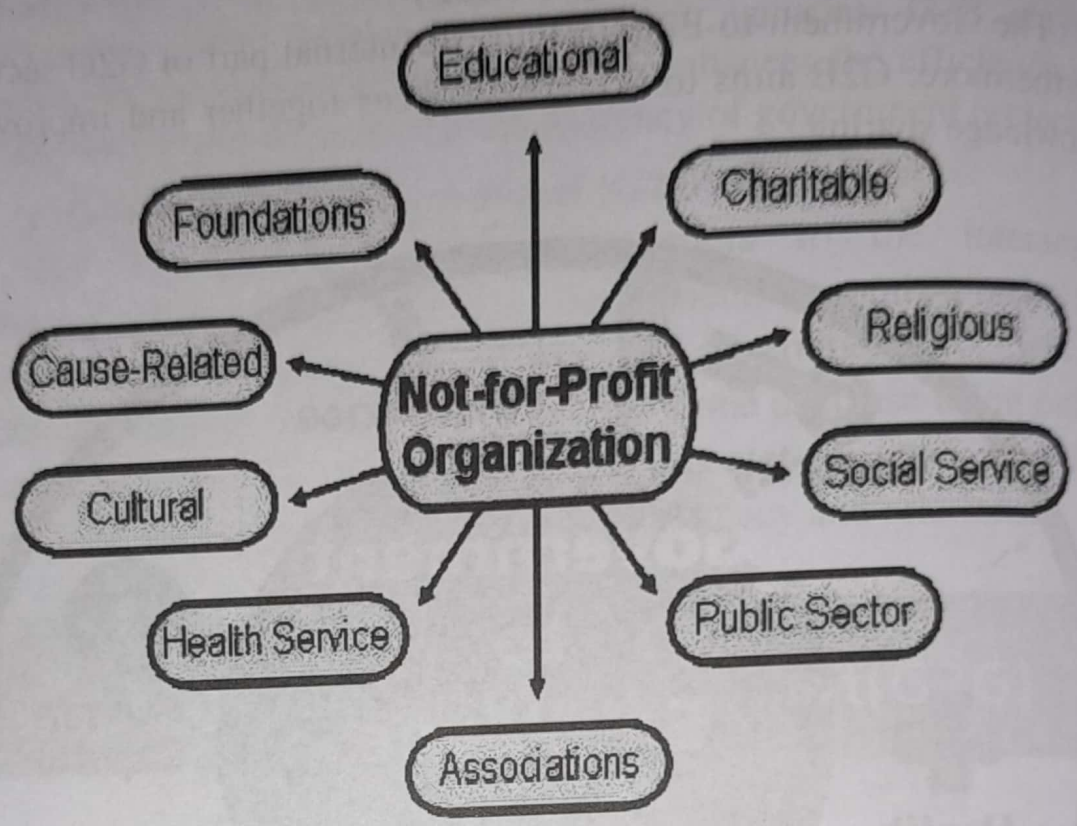
d. Government-to-Employee (G2E)

The Government-to-Employee is the internal part of G2G sector. Furthermore, G2E aims to bring employees together and improvise knowledge sharing.



Similarly, G2E provides online facilities to the employees. Likewise, applying for leave, reviewing salary payment record. And checking the balance of holiday. The G2E sector provides human resource training and development. So, G2E is also the relationship between employees, government institutions, and their management.

e. G2N (Government-to-Non-for-Profit Organisation)



7. E-Government Objectives

- **a.** Improve the internal organizational processes of governments
- **b.** Provide better information and service delivery
- **c.** Increase government transparency and accountability in order to reduce corruption
- **d.** Citizen easy access to government public information
- **e.** Simplicity, efficient, cost-effective and responsive governance
- **f.** Reinforce political credibility and accountability
- **g.** Encourage democratic practices through public participation and consultation

8. Existing ICT infrastructure and advantages :

- **a.** Submarine Cable connectivity 43.8 Gbps
- **b.** Bangladesh Railway optical fiber line
- **c.** Communication and Information Technology policy 2006

d. Established gov.bd domain for all ministries and government office
e. Bangladesh Computer Council
f. High-Tech park at Kaliakur
g. ICT incubator in Kawranbazar
h. Country-wide telecommunication infrastructure
i. Power Grid Company of Bangladesh (PGCB) fiber line
j. Secretariat backbone
k. Voter Database –Bangladesh Election Commission

9. Policy and Regulatory Framework

a. The Telegraphy Act, 1885[1]
b. The Wireless Telegraphy Act, 1933[2]
c. The National Telecommunication Policy, 1998
d. Copyright Act enacted with inclusion of Software and ICT, 2000
e. First ICT Policy drafted 2001
f. National ICT Policy adopted 2002
g. ICT Act, 2006 enacted
h. Revised Policy Drafted 2008
i. New ICT Policy approved 2009
j. ICT Act 2006 amended 2009
k. Rules for Digital Signature (Certifying Authority),2010
l. International Long Distance Telecommunication Services (ILDTS) Policy 2007 & 2010

10. E-Governance and ICT Act of Bangladesh

The "Information and Communication Technology Act, 2006," a Bangladeshi ICT law, allows for the use of Digital Certificates for document signing. The legislation established the Controller of Certifying Authorities and required Certifying Authorities to be

1. Act no XII of 1885
2. Act no XVII of 1933

licensed. The ICT Law specifies the processes that Certifying Authorities must follow. The Act specifies the legal enforcement and proper jurisdiction. There is a provision for the establishment of a special tribunal to handle this kind of lawsuit.

This legislation establishes the validity of Digital Certificates. The "Information Technology(Certifying Authorities) Rules, 2010" were drafted under the Act and are known as "Information Technology(Certifying Authorities) Rules, 2010." This document contains recommendations, guidance, and information regarding the elements that the CCA will consider in its operations and the Certifying Authorities' operations. The ICT legislation establishes legal recognition for electronic documents, as well as a framework to enable e-filing, e-commerce, and m-commerce transactions, as well as a legal framework to prevent and mitigate cybercrime.

The ICT Act facilitates the Trust Chain for public key infrastructure. The law enables the Controller of Certifying Authorities (CCA) to build up digital certificate infrastructure and manage it, including performing audits.

The ICT legislation was drafted to aid Bangladesh's growth of information and communication technology. Its goal is to make it easier to use information and communication technology to the construction of an information society.

When a document's contents are deemed private by law, confidentiality must be maintained using methods suitable to the mode of transmission, including via a communication network. Documentation outlining the agreed-upon method of transmission, as well as the safeguards in place to preserve the sent document's secrecy as evidence.

The Act was passed to provide information and communication technology legal legitimacy and security, as well as to create rules in this area.

The purpose of this Act is to ensure the legal security of documentary communications between individuals, partnerships, and the state, regardless of the medium used; the consistency of legal

rules and their application to documentary communications using media based on information technology; and the consistency of legal rules and their application to documentary communications using media based on information technology, whether electronic, magnetic, optical, wireless, or based on a combination of technologies; the functional equivalence and legal value of documents, regardless of the medium used, and the interchangeability of media and technologies; the linking of a person, a partnership, or the State with a technology-based document by allowing them to be identified by certification; and for the harmonization of media and technologies.

CHAPTER TEN
Privacy Protection and Cyber Security

1. Introduction

Because "cyberspace" has become such an important part of the global information and communication infrastructure, cyberspace security has become a top concern for businesses and governments across the globe.[1] According to the Cyber Security Act of 2015[2] *cyberspace* is "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship. The term "cyber security", though not defined in the *strategy*, is generally understood to encompass any measures taken to protect online information and secure the infrastructure on which it resides.[3]

Technologies that are ubiquitous, interconnected, and allow easy access to the Internet have become deeply integrated in everyday life. As a result, people are increasingly being dependant on cyberspace for social, economic and political interactions. The web

---

1. Deibert, Ron. Distributed Security as Cyber Strategy : Outlining a Comprehensive Approach for Canada in Cyberspace, Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012, Last visited on 25.08.2015
2. Bangladesh Government is to enact a new cyber security law with provisions for tough penalties for cyber crimes. The law will be a compliment to the existing Information & Communication Technology Act of 2006.
3. There is no commonly recognized definition for cyber security. ISO (ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. /IEC 27032/2012 defines cyber security as the "preservation of confidentiality, integrity and availability of information in the Cyberspace."

provides a platform for a whole range of critical infrastructure sectors and services, such as health care, food and water, finance, information and communication technology, public safety, energy and utilities, manufacturing, transportation and government.[1] Cyberspace connectivity augments all of these critical infrastructure sectors and is therefore vital to Bangladesh's future economic growth.

As the online environment has increasingly been subjected to sophisticated and targeted threats; the ever-increasing reliance on cyberspace is creating new and significant vulnerabilities.[2] This risk is magnified by a number of factors : more valuable electronic data is being stored and processed on a massive scale, much of it in the cloud; powerful and portable computing devices such as Smartphone's, tablets and laptops are increasingly integrated into every aspect of our lives; information is shared, combined and linked with other information with greater frequency; and third-party relationships e.g. outsourcing to a cloud provider, are the norm. Unless all components are equally secure, the entire system is vulnerable as cyber criminals are often skilled in exploiting weaknesses in cyberspace.

Privacy protection and cyber security should be thought of as interconnected : as more and more personal information are processed or stored online, privacy protection increasingly relies on effective cyber security implementation by organizations to secure personal data both when it is in transit and at rest.[3] In some cases, cyber security measures underpin critical infrastructure that protects data, thereby safeguarding personal information. However, as with many security measures, certain cyber security efforts can also threaten privacy; the relationship between cyber security and privacy

---

1. Public Safety Canada's website for list of critical infrastructure sectors,(Accessed on 27.08.2015).
2. This is acknowledged in the *Action Plan 2010-2015 for Canada's Cyber Security Strategy (the Action Plan)*, Released April 2013.
3. New Platforms, New Safeguards : Protecting Privacy in Cyberspace (February 23, 2011), https ://www.priv.gc.ca/media/sp-d/2011/spd_20110223_cb_e.asp (Accessed 27August 2015).

is not a completely harmonious one. Cyber security activities can require up-to-the-second monitoring of activities on a network in order to detect anomalies and threats, and in some cases, monitoring of this nature could involve capture and analysis of massive amounts of personal information.

2. Privacy and Cyber Security Issues in Bangladesh

"By allowing the production of enormous quantities of transactional data by and about people, the Internet has enabled the development of numerous possibilities for communication and information exchange. Individuals' personal information, their location and online activities, and logs and associated information about the e-mails and messages they send or receive are all included in this data, which is known as communications data or metadata." This communication data is "storable, accessible, and searchable," and it may be "both extremely revelatory and intrusive" when pooled and aggregated and utilized by the government."[4]

Ever since electronic media were opened to private sector involvement in the early 1990s, successive Bangladeshi governments have encouraged the development of an open internet access and communication regime in the country. Bangladesh currently has 33 million internet users, representing almost 20% of the total population, and ranks 138th out of 190 countries in the Household Download Index compiled by Net Index.[5] The World Economic Forum's 2013 Global Information Technology Report[6] ranked Bangladesh 114th out of 144 countries worldwide, with poor scores for its infrastructure and regulatory environment, even though an affordable and competitive communication service is generating exponential growth for users. In addition, localisation and the

---

4. Frank La Rue, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, in his landmark report on state surveillance and freedom of expression during the 23rd session of the UN Human Rights Council in Geneva in April 2003.
5. www.netindex.com/download/allcountries(accessed 3May 2015).
6. www.weforum.org/reports/global-information-technology-report-2013(accessed 3May 2015).

availability of phonetic Bangla software have contributed to the development of local blog and content hosting services.[7] The current Government in Bangladesh has a plan to establish what it calls a "Digital Bangladesh by 2021", with the aim of integrating internet access with development efforts in various sectors; but with widespread digital communication comes a greater threat to security and privacy, and uncertainty on how state and other institutions will address those issues while protecting the rights of individuals.

Globally there are two models available to protect citizens. One is the authoritarian model, where the problem is addressed through the development of a surveillance regime with filtering at the control points or on the backbone of the internet, and monitoring of the use of computers. A more liberal approach, on the other hand, is to make people aware of the risks, to develop their capacities and to set down punitive measures that require proper evidence and respect individual rights.[8] Bangladesh is often swinging between these two models, and there is a sense in which it is addressing the situation on an ad hoc basis.

3. Status of Bangladesh ICT Policies & Security Challenges

The Government of Bangladesh has established the National Council for Science and Technology in order to enhance the living standards of the general public by expanding development efforts in science and technology and their application (NCST). The Council's Executive Committee has also been established to carry out the Council's policies.

Recently formulated National Information and Communication Technology Policy (2002) has also given enormous importance to the development of ICT[9] for capturing people's share in the multi-

---

7. *Freedom on the Net 2013 : Bangladesh*, www.freedomhouse net/2013/bangladesh#.U4aWAfldXsF.org/report/freedom,(accessed 4May 2020).
8. M. Hassan, (2012, June 30). 'Cybercrime : Implementation must to achieve Vision 2021,' *The Daily Star*, available at archive thedailystar.net/law/2012/06/05/ analysis.htm,(accessed 11 August 2019).
9. Information and Communication Technology be abbreviated as ICT throughout the chapter of the study.

billion dollar software export market, for ensuring good governance, for enacting ICT related policies, special allocation of funds for software projects, development of world class ICT professionals and creation of a world class ICT institution for promoting excellence in the field.

By the year 2006, the Vision of this Policy 2002 is to create an ICT-driven country with a knowledge-based society. To achieve this goal, a country-wide ICT infrastructure was to be developed to ensure that every citizen has access to information, thereby facilitating citizen empowerment and enhancing democratic values and norms for long-term economic development through the use of infrastructure for human resources development, good governance, e-commerce, banking, public utility services, and other on-line ICT-enabled services.

Human resource development, the construction of ICT infrastructure, supporting ICT research and development, and the growth of ICT industries are all addressed in the 2002 National ICT Policy. It also emphasizes the importance of hardware industries, e-commerce, e-governance, ICT legal issues, ICT application in health care, and ICT application in agriculture to maximize the potential for rural economy and agro-business development. The use of ICT in other areas such as social welfare, transportation, and the legal system is also discussed.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL)[10] has adopted a Model Law on Electronic Commerce. This is known as UNCITRAL Model Law of e-commerce. In conformity with UNCITRAL Model Law, Bangladesh drafted an ICT Law, which has been approved by the parliament in February 2005 to facilitate electronic commerce and to encourage growth and development of information technology.

The ICT Law establishes rules and norms that validate and recognize contracts, forms through electronic means, sets default

10. The United Nations Commission on International Trade Law may be called UNCITRAL through the study.

rules for contract formation and governance of electronic contract performances, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes and supports the admission of computer evidence in courts and arbitration proceedings. In addition, the Copy Right Act 2000 has been amended to include computer software.

The Government is committed to mounting a direct and sustainable effort on the reduction of poverty, enhancing livelihood security, removal of hunger and malnutrition and generation of employment. This calls for generation and screening of all relevant technologies, their widespread dissemination through networking and support for the vast unorganized sectors of the economy of the country.

Realizing the importance of ICT and the enormous impact it can create in our everyday life, the name of the Ministry has been changed from Ministry of Science and Technology to the Ministry of Science and Information & Communication Technology. The Ministry of Science and ICT have been entrusted with the responsibility of harmonious growth of this sector in Bangladesh. Bangladesh Computer Council (BCC)[11], the apex body having the responsibility for promotion of all sorts of ICT activities in the country, is also governed by the Ministry of Science and ICT.

Development of Science and ICT depends on the expansion of telecommunication sector. This sector is still under developed due to lack of deregulation and open competition. In 2002, independent telecom regulatory authority, Bangladesh Telecommunication Regulatory Commission (BTRC) has been created.

4. The Government Activities

Cyber diplomacy is one of the foreign policy priorities of Bangladesh's current Government. The Government is planning to

---

11. Bangladesh Computer Council (BCC), an organization established by the government that ensures the use of computers and information technology in order to achieve the necessary policies and activities.

enact cyber security law to ensure security of the Government services and protect its own information technology[12] system Bangladesh joined the just launched Global Forum on Cyber Expertise (GFCE)[13] at the Hague for promoting international cooperation on cyber security.

The Government of Bangladesh in collaboration with a global cyber security firm is going to develop a modern 'National Cyber Defence and Cyber Security Doctrine' to check the fast growing cybercrime, intellectual property theft, industrial espionage or IT infrastructure abuses. The development of modern cyber defence and cyber doctrine is to legitimate, inclusive and based on deep technological knowledge in order to improve Bangladesh's capacity to manage the risks related to digital revolution. Bangladesh's new economy, largely based on the development of IT industry, is expected to improve the socio-economic condition and livelihood of the people. The other supporting activities and deliverables include preparation of the government of Bangladesh Information Security Manual, report on Bangladesh Information Security Classification and Information Protection Tools, Telecommunication and ISPs[14] Information Security Manual, Cybercrime Legislation, Cyber security awareness campaign and consensus building as well.

5. Policy regarding Privacy and Cyber Security in Bangladesh

Communication content can reveal a range of sensitive information about an individual, including a person's identity,

---

12. The Information Technology (is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data) may be called IT through the study.
13. The GFCE ensures a flexible, action-oriented and consultative forum that can evolve to meet contemporary challenges in cyberspace. It reflects the shared understanding of its members that the GFCE should be structured in a way that is voluntary, complementary, inclusive and resource driven. Activities are focused on identifying and addressing key geographic and thematic cyber issues.
14. An ISP (Internet service provider) is a company that provides individuals and other companies' access to the Internet and other related services such as Web site building and virtual hosting.

behaviour, associations, physical and medical data, race, colour, sexual orientation, national origins and viewpoints. It can show trends in a person's location, movements, interaction or behaviour patterns over a period of time through metadata or other forms of data associated with the original content. Therefore, this requires significant protection in law.

Internationally, regulations concerning government surveillance of communications vary in approach and effectiveness, often with very weak or non-existent legal safeguards.[15] The Constitution of Bangladesh touches on the issues of privacy and individual security in several places. Article 11 says that the Republic shall be a democracy in which fundamental human rights and freedoms and respect for the dignity and worth of humans shall be guaranteed. Article 43 states that every citizen has the right to be secured in his or her home against entry, search and seizure, and the right to the privacy of his or her correspondence and other means of communication, unless there are any reasonable restrictions imposed by law in the interests of the security of the state.

In Bangladesh cyber crime is addressed with reference to several laws, including the Information and Communication Technology Act, 2006; the Penal Code, 1860; the Pornography Act, 2012; and the Bangladesh Telecommunication Act, 2001.

The Bangladesh Telecommunication (Amendment) Act, 2006, allows agencies to monitor the private communications of people with the permission of the chief executive of the Ministry of Home Affairs, under a special provision for the security of the State and public order. This Act was again amended in 2010, enabling officials to intercept the electronic communications of any individual or institution in order to ensure the security of the State or public order.[16]

---

15. K. Rodriguez, *Surveillance Camp IV : Disproportionate State Surveillance A Violationof Privacy*, 2013, Available at : Electronic Frontier htt ://www.eff.org/deeplinks/2013/02/disproportionate-state-surveillance-violation privacy(accessed 11July 2015).
16. https ://www.privacyinternational.org/reports/bangladesh/ii-legal-framework, (accessed 8 August 2015).

The Act was further amended in 2013 by granting law enforcers the right to arrest any person without warrant, and by making the crimes non-bailable. Section 57 of the Act states that if any electronically published material causes any deterioration of law and order, tarnishes the image of a person or the State, or hurts the religious sentiment of people, the offender is too punished for a maximum of 14 years imprisonment.[17]

The Bangladesh Telecom Regulatory Commission (BTRC)[18] also has the authority to tap and monitor phone calls if deemed necessary. The commission's International Long Distance Telecommunications System Policy[19] has enabled the country to set up three private international gateways, six interconnection exchanges and one international internet gateway. This policy says the operators of these will arrange the connection, equipment and software needed for online and offline monitoring, and will provide access for "lawful interception" by law enforcement agencies. All operators are also required to provide the records of call details (voice and data) whenever necessary. The BTRC may also set up a monitoring centre at the country's submarine cable landing station which connects Bangladesh's internet backbone to the rest of the world.

In January 2012, the BTRC created an eleven-member Bangladesh Computer Security Incident Response Team (BD-CSIRT) to look into the issues of cyber crime. This team was mandated to use wiretapping and internet surveillance if necessary. The Government has also set up a "Cyber Tribunal" accordingto

---

17. ICT (Amendment) Act, 2013 : *Right to Information and Freedom of Expression under Threat*, available at ASK. www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat, also available Daily Star, October 9, 2013.
18. The Bangladesh Telecommunication Regulatory Commission (BTRC) is an independent Commission founded under the Bangladesh Telecommunication Act, 2001 (Act no 18 of 2001). The BTRC is responsible for regulating all matters related to telecommunications (wire, cellular, satellite and cable) of Bangladesh.
19. Available at www.btrc.gov.bd /sites/default/files/ ildts_ policy _2010_ english - 0.pdf

Section 68 of the ICT Act of 2006 to deal with cyber crime-related issues. The Right to Information Ordinance of 2008 was modified and gazetted in 2009. This Ordinance has a provision for the proactive disclosure of information ensuring better transparency in the administration, but the amended ICT Act of 2013 may discourage the administration to disclose any information fearing the application of Section 57 of ICT Act.[20]

6. Cyber Security Challenges

The Internet is without a doubt the most significant technology of our day; its practical uses have not only made our lives simpler than ever before, but it also plays a critical role in education, entertainment, and commerce. It does, however, have certain drawbacks. For the criminal element of society, it has opened up a huge new universe. The most serious danger to the internet is a security breach. Cybercrime and security breaches are now projected to be worth a total of 105 billion dollars worldwide. As a result, cybercrime and cyber security must be given top attention.

7. The Problems with Cyber Security

The term "cyber security" often lacks clear definition. It is used as an umbrella concept covering a range of threats and responses[21] involving national infrastructure, internet infrastructure, applications and software, and users. Sometimes it is even used to refer to the stability of the state and political structures. The inexact terminology of cyber security "mixes legitimate and illegitimate concerns and conflates different types and levels of risk." This "prevents genuine objective scrutiny, and inevitably leads to responses which are wide-

---

20. M. S. Siddiqui, ICT Act and freedom of expression, *Financial Express*, September 29, 2013 available at www. thefinancialexpress bd.com. /old/index.php.
21. Centre for Democracy and Technology, Unpacking, "Cyber security" : Threats, Responses,andHumanRightsConsiderations. https ://cdt.org/insight/unpacking-cybersecurity-threats-responses-and-human-rights-considerations (accessed 21January2015).

ranging and can easily be misused or abused".[22] Cyber security not only leads to overly broad powers being given to the state, it also "risks generating a consensus that is illusory" and not useful for the problems at hand.[23] People of Bangladesh need to carefully unpack the relevant issues and develop "a clear vocabulary of cyber security threats and responses," so as to enable "targeted, effective, and rights-respecting policies".[24] If they do not, cyber security can be used by governments as a justification to censor, control or survey internet use.

Viewing cyber security as an issue of national security is perilous and unhelpful. People of Bangladesh should distinguish between, and not conflate, on the one hand, protecting computers, networks and information, and on the other hand using technological tools to achieve security objectives. Using "cyberspace as a tool for national security, both in the dimension of war fighting and the dimension of mass surveillance, has detrimental effects on the level of cyber security globally".[25] When cyber security is framed as a national security issue, issues regarding technology and the internet are *securitised* – brought onto the security agendas of states. This may be counterproductive. The state, law enforcement, military and intelligence agencies may not have the best skills or knowledge for the job. State actors may have a conflict of interest in securing information : militaries, for example, may want to develop offensive weapons, while intelligence agencies may rely on breaking or circumventing information insecurity in order to survey better. Cyber security may also be used to protect state secrets, and criminalise

---

22. A. Kovacs and D.Hawtin, 'Cyber Security, Surveillance and Online Human Rights,'*Discussion paper written for the Stockholm Internet Forum*, 27-28 May, 2014, available at www.gp-digital.org/publication/second-pub(accessed 12 December 2014).
23. Non-governmental Perspectives on a New Generation of National Cyber security Strategies, p. 6. Available at dx.doi.org/10.1787/5k8zq92sx138-en
24. On this point may seen Centre for Democracy and Technology.
25. M. D. Cavelty, 'Breaking the Cyber-Security Dilemma : Aligning Security Needs and Removing Vulnerabilities', *Journal of Science and Engineering Ethics*, vol3,2014, pp.701-715.

whistleblowers as cyber security threats. Focusing on the state and "its" security, "crowds out consideration for the security of the individual citizen, with detrimental effects on the security of the whole system."[26]

Cyber security often disproportionately focuses on the protection of information, databases, devices, assets and infrastructures connected to the internet, rather than on the protection of connected users. Technological infrastructures and the assets of corporations are put at the centre of analysis, rather than human beings. Human beings are seen as a threat in the form of bad "hackers" or as a weak link in information systems, making mistakes and responding to phishing or "social engineering" attacks.[27] Putting humans at the centre of cyber security is important. A definition of cyber security as purely protecting information avoids ethical challenges. Cyber security should not protect some people's information at the expense of others. It should also not protect information about state secrets in order to enable mass surveillance and privacy invasion of individual users.

A report from the World Economic Forum released in January 2014 examines the need for new approaches to increase resilience against cyber attacks and suggests that the failure to effectively secure cyberspace could result in an aggregate impact of approximately US$ 3[28] trillion by 2020.[29] However, many of the challenges for cyber security are also challenges for privacy and data protection. Cyber security is by no means a static issue with a permanent solution. Threats to information in cyberspace evolve quickly and, more recently, have expanded into new channels such as social media and mobile technologies. As organizations strive to keep pace with the changing landscape created by innovative technologies, social practices and ever-changing threats, data

---

26. Ibid.
27. D. Cavelty, . op cit. defines social engineering as "psychological manipulation of people into performing actions or divulging confidential information.
28. The currency of the United States is called US Dollar that is marked as US$
29. World Economic Forum report on *Risk and Responsibility in a Hyperconnected World*, released January 20, 2014.

produced, collected and collated on a massive scale can be left vulnerable to those cyber threats. The following are some of the emerging challenges for data protection and cyber security.

8. Complexity of the Connected Environment

The continuing evolution of cyberspace, as a fully electronic world created by interconnected networks in parallel with our physical environment, is characterized by an enormous amount of data. The modern economy increasingly depends on vast quantities of digital data that are generated through financial transactions, communications, entertainment, travel, shopping, online browsing, and hundreds of other routine activities.[30] Data elements are continually being combined, connected, compared and linked to other information as organizations try to capitalize on its value and to offer new and improved services to their users. The electronic systems and digital networks that facilitate these transactions and communications also capture preferences and other personal details, and track online and, increasingly, physical movements. The volume of data generated in cyberspace can only increase exponentially once the "Internet of things" becomes a reality, and sensors within devices autonomously report on location, status, surrounding environment, provide real-time updates or help monitor and control devices remotely.[31]

Cyberspace has become inherently complex to manage and challenging to secure. Increased, persistent connectivity through a greater range of mobile devices and "always on" services, third-party business relationships, cloud computing infrastructures, information sharing agreements, and other "seamless" or automated business processes in cyberspace continue to pose shared risks to cyber security and privacy. Threats in cyberspace are to continue to target the weakest links in any complex web of business relationships or

---

30. Center for Applied Cyber security Research, Indiana University. *Roundtable on Cyber Threats, Objectives, and Responses : A Report*. December 2012.
31. Business Insider "*Everything You Need To Know About The New Internet-The 'Internet Of Things'*, Julie Bort, Published March 29, 2013,(Accessed 17August2015).

government processes, meaning stakeholders in cyber security efforts have a shared role in protecting the infrastructure and the information that flows through it.

9. Growing sophistication of the Threat

Online threats may be invisible but their effects are very real, and interconnected systems that are globally accessible are inherently vulnerable. As the scale of information flowing through cyberspace has expanded, so too has its value to corporations, government, and those with malicious intent. Data trails now leave a larger footprint across cyberspace, leaving people more exposed to threats. Wherever there is an opportunity to profit there is usually a market for criminal activity, but as Gabriella Coleman notes, there has also been a "professionalization" of hacking[32] and cyber-crime, making these activities much more sophisticated. State-sponsored threats, conducted or condoned by a nation state, are also becoming increasingly common. These are sometimes referred to as Advanced Persistent Threats and are usually well educated, well resourced adversaries who focus on the theft of secrets including intellectual property.[33]

The cyber-crime is growing in frequency and complexity for several reasons : "First, the number of users coming online, including individuals, businesses, organizations, and governments, is growing rapidly, creating a growing baseline of potential targets. Second, the ways in which people communicate and share information online has changed fundamentally over the last several years, with the growth of social networking, cloud computing and

32. "Hacking" is the commonly used term, however the technically correct term is "cracking" - a shortened form of "criminal hacking". Hacking, in the original sense of the word, is figuring out how things work. Where the term "hacking" is used throughout the paper, it is meant to refer to criminal hacking activities, aka "cracking". For more on hacking, see the work of Gabriella Coleman; in particular, Politics and Public or Hacker Practice : Moral Genres and the Cultural Articulation of Liberalism.

33. 'Study of the Impact of Cyber Crime on Businesses in Canada,' *International Cyber Security Protection Alliance*,2013, p. 33.

mobile forms of connectivity. People share more data with each other, entrust it to third parties outside our immediate control, and click on links and documents over social networking platforms and services with a greater degree of frequency. Third, the companies rarely disclose security breaches to the public for competitive and reputational reasons, there is limited information about how attacks are carried out, which could ultimately hinder cyber security efforts.

10. Threats Moving to the Mobile Sphere

Mobile devices can contain a goldmine of personal information. People routinely carry their mobile devices everywhere and use them for almost anything imaginable; people communicate with friends, access email, take photos and video and upload it to the web, play games, track distances, locate nearby stores and restaurants, find directions to specific locations, access their bank accounts, surf the web, monitor their health/physical activity, keep track of appointments or log to-do lists. Organizations are all striving to reach consumers and clients on the devices they use every day, but alongside all of these conveniences for the consumer is the possibility for new vulnerabilities or opportunities for cyber threats.

The International Cyber Security Protection Alliance (ICSPA)[34] recently released a cyber-crime study that highlighted mobile communications and cloud services as today's new targets for the cyber-criminal. The study notes that one of the significant concerns facing the mobile industry is how to address the skyrocketing amount of malware on mobile devices. Malware[35] can easily be distributed to mobile devices through malicious apps within smart

34. The International Cyber Security Protection Alliance (ICSPA) was established to channel funding, expertise and assistance directly to assist law enforcement cyber crime units in both domestic and international markets. ICSPA is a business-led organisation comprising large national and multi-national companies who recognise the need to provide additional resourcing and support to law enforcement officers around the world, in their fight against cyber crime.
35. Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems

phone app stores which appear safe. Furthermore, the use of free public Wi-Fi[36] can also put mobile devices at increased risk of having data intercepted. ICSPA's study concludes that mobile malware is a key emerging threat in cyberspace. Although it has been argued that cyber criminals are building better malware specifically designed for mobile devices, actual infection rates on devices are low, for the present, since the distribution of malware to mobile devices has not yet been perfected.[37] This can be expected to change in the near future.

As cyber threats increasingly target mobile devices, data protection becomes all the more critical. Communications and transactions using mobile devices are more closely tied with individual users, sensors within mobile devices can be enabled to locate devices with a high degree of precision, and features built into the devices or apps that people download can track, record and store personal information, upload contact lists, communications and transactions. Faced with these mounting risks, the mobile industry, companies and app developers have a heightened responsibility to ensure the safety of the platforms and the backend systems, where so much personal information are collected, handled and stored.

11. Compliance vs. Risk-Management

Organizations are required to comply with various laws and regulations in order to operate in particular jurisdictions or across various jurisdictions. When it comes to security, however, a mechanical approach to compliance does not necessarily mean that the organization is secured. In fact, blindly pursuing compliance may

36. Wi-Fi is a technology that uses radio waves to provide network connectivity. A Wi-Fi connection is established using a wireless adapter to create hotspots - areas in the vicinity of a wireless router that are connected to the network and allow users to access internet services.
37. This argument is based on the view that most Android malware is found hidden in apps sold or given away for free in online stores other than the official Google Play store, which scans for malicious code. Computerworld 'Windows malware finds its way to Android', by Antone Gonsalves, published August 16, 2013,(Accessed 4 October 2014).