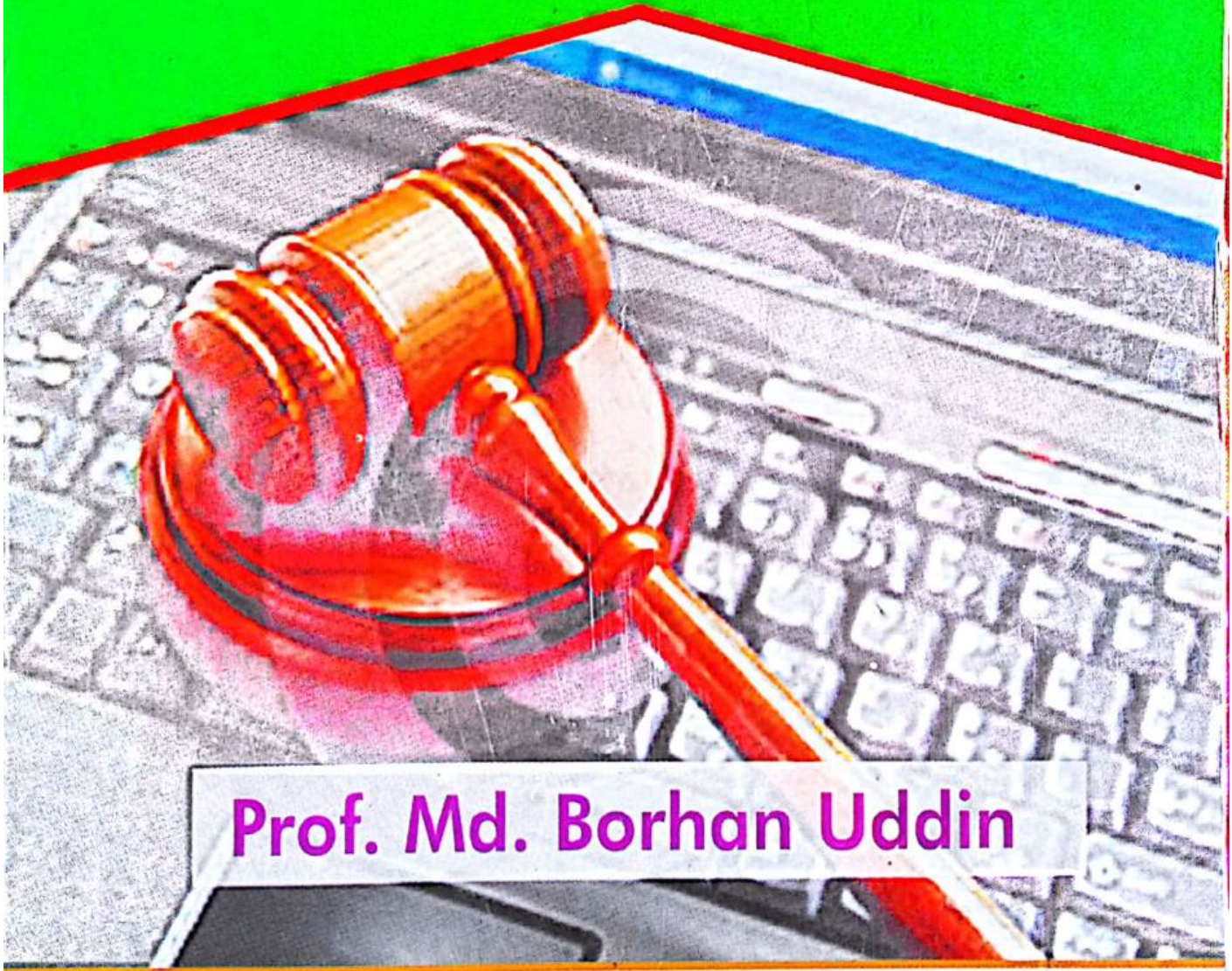
PRINCIPLES OF CYBER LAW

&

OTHER RELATED LAWS



Prof. Md. Borhan Uddin

SHAMS PUBLICATIONS

CONTENTS of
Principles of Cyber Law

CHAPTER-1
Cyber Law

CHAPTER – 2
Cyber Jurisprudence & Human Rights

CHAPTER – 3
Internet and Networks

CHAPTER – 4
Cyber Crime

CHAPTER – 5
Tools and Techniques of Cyber Crime

CHAPTER – 6
Hacking

CHAPTER – 7
Cyber Terrorism

CHAPTER – 8
Cyber Threat to Critical Infrastructure

CHAPTER – 9
Computer Port Scanning Protocol

CHAPTER – 10
Cyber Crime and International Laws

CHAPTER – 11
Virus

CHAPTER – 12
Worms

CHAPTER – 13
Trojans

CHAPTER – 14
Cyber Forensics and Investigation

CHAPTER – 15
Digital Evidence
E-Evidence

CHAPTER – 16
Cyber Crime Cases

CHAPTER – 17
E-mail related crime

CHAPTER – 18
Digital Signature, Electronic Signature, Cryptographic Signature

CHAPTER – 19
Cyber Vandalism

CHAPTER- 20
Cyber Chat or Chatting

CHAPTER – 21
Short Notes

CHAPTER – 22
E-Commerce
M-Commerce

CHAPTER – 23
E-Governance

CHAPTER – 24

E-Readiness

E-Readiness: Bangladesh Perspective.

CHAPTER – 25

E-learning

CHAPTER – 26
E-journal

CHAPTER - 27
Internet Service Provider (ISP)

CHAPTER – 28
Electronic Media

CHAPTER- 29
Computerization in Bangladesh

Statutory Cyber Laws

Chapter–1
Cyber Law

1. Introduction of Cyber law

Cyber law is a law related to Information Technology (IT) and Information and Communication Technology (ICT). Cyber law is a new phenomenon of modern technological development. Information Technology (IT) very rapidly occupied the responsibility of development of human society. Internet is a new and most influential concept of IT. It has rendered a tremendous prospective aspect for the human civilization. Internet technology is growing in an unplanned and unregulated manner. The inventors of this new technology may not really anticipate the scope and far reaching consequences of cyberspace.

The growth rate of cyberspace has been enormous. It is growing rapidly with the population. Cyberspace is the newly expected environment of the world. Due to the spontaneous and phenomenal growth of cyberspace, various legal aspects arise. It is absolutely a complex subject. Newly emerging legal issues are being related to cyberspace. So Cyber Law or the Law of Internet is required to be enforced. The growth of Cyberspace has resulted in the development of a new and highly specialized branch of law called Cyber Laws. This is the Law of the Internet and the Law of World Wide Web (www). So Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web (www).

2. What is Cyberlaws?

Cyber Law is the law governing computer and the Internet. Today's highly digitalized world, almost everyone is related with the cyber law. Sky-Civilization influenced over the human society of the world tremendously through digitalized Information and Communication Technology (ICT). Cyberspace, Satellite Station, Satellite Broadcast. Internet, World Wide Web (www) etc are the blessings of modern scientific and technological development. The scope of the IT is so vast and striking that almost all the people of the world is under one network. The life becomes comfortable and the whole world comes under the grip of hand.

Cyber crime cases are related with online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, email hijacking, denial of service, hacking, pornography, defamation, sale of illegal products etc are becoming common. Digital signatures and E-contracts are fast replacing conventional methods of transacting business.

This present emerging contribution of the science should be regulated by law for the better interest of the human society and civilization. So

"The law related to control the behavior, rights, duties and obligations of the beneficiaries of Satellite Station, Satellite communication, internet, cyberspace, Information and Communication Technology (ICT) etc is termed as Cyber Law."

3. Definition of Cyber Law

According to Wikipedia, the free encyclopedia,

"Cyber law is a term used to describe the legal issues related to use of communications technology, particularly cyberspace, i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world."

4. What is Cyberspace?

Cyberspace is a new concept of modern Information and communication Technology (ICT) world. It is the metaphorical space of computer systems and computer networks. In this space electronic data are stored and online communication takes place. The term was originated in science fiction. It includes various kinds of virtual reality by computer users or by entities who uses computer System.

The cyberspac is a new word and a new concept of space. Cyberspace is an apparent perception of object experienced daily by the operators of Information Technology and Information and Communication Technology through out the world. It is a complexity beyound immagination. It is the conception regarding the nonspace of mind, clusters and assemblage of data.

The word Cyberspace is connected with computer and telecommunications networks system. It is a silent world. It is the place where communication, conversation and data transfer appears to occur. It is an immense region of electron states, microwaves, magnetic fields and light pulses. It is named as Cyberspace by IT adminstration.

5. What is Internet?

The Internet is a worldwide communication network. It is publicly accessible network of interconnected computer networks. It transmits data by packet switching using the standard Internet Protocol (IP). It is a network of networks. It consists of millions of smaller domestic, academic, business, and government networks. These together carry various informations and services, such as electronic mail, online chat, file transfer, and the interlinked Web pages and other documents of the World Wide Web (www).

6. What is Intellectual Property?

Intellectual property (IP) is a term for various legal entitlements. It includes written text, recorded media and inventions. The holders of

these legal entitlements are entitled to exercise various exclusive rights in relation to the subject matter of the IP. The term intellectual property reflects the idea that it is the product of the mind or the intellect.

The enforcement of Intellectual Property Laws varies from jurisdiction to jurisdiction. Inter-governmental efforts are essential to harmonise the law through international treaties. Intellectual Property Rights (TRIPs) is a legal right. Intellectual property laws confer a bundle of exclusive rights in relation to the particular manner of IP. The term intellectual property denotes the specific legal rights which authors, inventors and other IP holders may hold and exercise.

7. What is Privacy?

According to Dictionary Privacy means : seclusion : a place of seclusion : retreat : retirement : avoidance of notice or display : secrecy: a private matter: The quality of being secluded from the presence or view of others: The condition of being concealed or hidden.

Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known. Privacy can be seen as an aspect of security.

The right against unsanctioned invasion of privacy by the government, corporations or individuals is a part of many countries' laws and in some cases, constitutions or privacy laws. Almost all countries have laws which limit privacy. For example taxation normally requires passing on information about earnings. In some countries individual privacy may conflict with freedom of speech. Some laws may require public disclosure of information in some countries. But it may be considered private in other countries and their cultures.

8. What is Internet Privacy?

Internet privacy means the privacy of computer and server and related systems. Internet is an assemblege of privately and publicly owned servers and computers. These systems are able to retain data. It is able to save or retain the fact. Use of privacy software or reliance upon a proxy server, it may increase the level of personal privacy protection of a user on the Internet. A user's own computer may store data. Internet privacy involves with the erosion of security through web search engines. It provides increased access to personal information

online. These are public records, social networking profiles, biographical webpages or online resume. To protect these flow of informations internet privacy is required.

9. Privacy from government interference:

Generally Government interfear the privacy of persons. Privacy of human right basically relates to government actions, not private actions. Human rights guarantees do not impose broad obligations on governments to protect individuals privacy. Constitutional and international guarantees require the restrictions on freedom of expression. Privacy has legality and necessity. In many countries Governments are empowered to breach privacy. In case of criminal investigations, police are permitted to search for and seize private property from any places though it is prohibited to enter their without permission.

Information being transmitted over a phone line is secretly monitored by Law Enforcement Agencies. It is usually requires permission from a court. This can be used as evidence in trials. It is used to secure convictions against criminals. Individuals conducte are monitored by closed-circuit television cameras. These are placed in public places. Also forward looking infrared cameras are mounted on police helicopter to monitor public activity.

The right to privacy is a human right. It is up to the person whether they should disclose information or not. Government agencies like the National Security Agency are in opinion that the ability to monitor all communications aids in the prevention of criminal activity and terrorism is nesessary.

10. Effect of war upon privacy:

During periods of war, identity documents and similar artifacts have been introduced to establish the identity of the holder. These were used for security purposes. Individuals who did not carry the required documents were assumed to be spies and could be interrogated. In World War-1 identity cards were introduced in the United Kingdom. In 1919 compulsion to carry them was removed. They were reintroduced in World War II. Chief Justice Lord Goddard commented that identity cards tend to make people resentful of the acts of police.

Rights of the individual, including habeas corpus, often only apply in periods of peacetime. During the American Civil War in the United States, and during World War II in the United Kingdom, habeas corpus

was suspended. It is the opinion of some that the September 11, 2001 attacks and the War on Terrorism declared by the United States government, has reduced the right to privacy.

The United Kingdom Labour Government introduced the Identity Cards bill in 2005, Bill. This bill create a national identity database and introduce a national identity card. The idea was initially revived after the 11 September, 2001 attacks. It became the part of Labours Manifesto for the 2005 general election. As of 2006, the right to privacy remains an important point of political debate in the United States, the United Kingdom, and other countries also in Bangladesh.

11. Constitutional basis of privacy; Invasion of Privacy:

Amendment IV (the Fourth Amendment) to the United States Constitution is one of the provisions included in the Bill of Rights. The Amendment guards against unreasonable searches and seizures, and was originally designed as a response to the controversial writs of assistance (a type of general search warrant), which were a significant factor behind the American Revolution.

The Fourth Amendment to the United States Constitution requires that searches and seizures conducted under governmental authority be "reasonable". Toward that end, the amendment specifies that judicially sanctioned search and arrest warrants must be supported by probable cause and be limited in scope according to specific information supplied by a person (usually a peace officer) who has sworn by it and is therefore accountable to the issuing court.

The amendment applies only to governmental actors; it does not guarantee to people the right to be free from unreasonable searches and seizures conducted by private citizens or organizations. More specifically, the Bill of Rights only restricts the power of the federal government, but the Supreme Court of the United States has ruled that the Fourth Amendment is applicable to state governments by operation of the Fourteenth Amendment.

The Supreme Court has said that some searches and seizures may violate the Fourth Amendment's reasonableness requirement even if a warrant is supported by probable cause and is limited in scope. Conversely, the Court has approved routine warrant less seizures, for example "where there is probable cause to believe that a criminal offense has been or is being committed." Thus, the reasonableness requirement and the warrant requirement are somewhat distinct.

Regarding the Fourth Amendment's reasonableness requirement, it applies not just to a search in combination with a seizure, but also applies to a search without a seizure, as well as to a seizure without a search. Hence, the amendment is not limited to protecting elements of privacy or personal autonomy, but rather applies pervasively to virtually all aspects of criminal law. Nevertheless, the amendment is not so broad as to replace other constitutional provisions, such as replacing the Eighth Amendment's ban on "cruel and unusual" punishment with a more sweeping ban on "unreasonable" punishment.

The Fourth Amendment was needed because the writs of assistance had alarmed the country, and had inspired citizens to demand their rights. Congress recognized those demands, and so we have the Fourth Amendment today. But does the word "unreasonable" mean unreasonable according to the people of 1789, or according to people today, or according to judges, or according to juries? This question has not been definitively answered. However, to the extent that the Fourth Amendment is used for purposes of striking down statutes, the framers expected that the standard of review would be clear and irreconcilable variance with the Fourth Amendment

12. What is Freedom of Speech?

Freedom of speech is the concept of the inherent human right. Persons can pass their opinion publicly without fear of censorship or punishment. The right is preserved in the United Nations Universal Declaration of Human Rights. It is granted formal recognition by the laws of most nations. In many nations, government censorship is enforced. There are different approaches of law to the issues such as hate speech, obscenity, and defamation laws.

Freedom of speech guranted as fundamental right, under Article 39 of the Constitution of the People's Republic of Bangladesh. The Article states that,

1. Freedom of thought and conscience is Guranted.
2. Subject to any reasonable restrictions imposed by law in the interests of the security of the state, friendly relation with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence-
   a. the right of every citizen to freedom of speech and expression; and
   b. Freedom of the press are guranted.

13. What is Jurisdiction?

According to Chamber dictionary Jurisdiction means : the distribution of justice : legal authority : extent of power : district over which any authority extend :

According to law, ' jurisdiction is the practical authority granted to a formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and, by implication, to administer justice within a defined area of responsibility.'

As a topic, jurisdiction draws its substance from Public International Law, Conflict of Laws, Constitutional Law and the powers of the executive and legislative branches of government to allocate resources to best serve the needs of its native society. There are three main types of judicial jurisdiction-

1. Personal jurisdiction (personam): Authority over a person regardless of his location.

2. Territorial jurisdiction(locum): Authority confined to a bounded space, including all those present therein, and events which occur there.

3. Subject matter jurisdiction (subjectam) : Authority over the subject of the legal questions involved in the case.

A court must have a concurrence of subject matter jurisdiction with either personal or territorial jurisdiction. The territorial jurisdiction is critical, on the principle that courts enforce laws which are territorial in their authority.

14. What is Censorship:

Censorship is the power of removal or withholding of information from the public by a controlling group or body. The censorship is generally imposed by governments, religious groups, or the mass media. There are other forms of censorship exist. Official secrets, commercial secrets, intellectual property, and privileged lawyer-client communication is not usually described under censorship, when it remains within reasonable bounds. The term censorship often carries a sense of untoward, inappropriate or repressive secrecy.

Censorship is closely related to the concepts of freedom of speech and freedom of expression. It is often associated with human rights abuse, dictatorship, and repression. The term censorship is often used to signify a belief that a group controlling certain information improperly or for its own benefit, or preventing others from accessing information that should be made readily accessible.

15. What is Nature of Cyberlaws?

The nature of the Cyber law can be described under the following aspects.

A. Jurisdiction and sovernity of Internet
B. Net Neutrality
C. Free Space in Cyberspace
D. Internet Regulation In different Countries

A. Jurisdiction and sovernity of internet

The Internet does not tend to make geographical and jurisdictional boundaries. But Internet users are remaining under physical jurisdictions. These are

The laws of the state in which the user resides,

1. The laws of the state that apply where the server hosting the transaction is located, and
2. The laws of the state which apply to the person or business with whom the transaction takes place.

So a single transaction may involve the laws of at least three jurisdictions. For Example a internet user of Bangladesh conducting a transaction with another user in china through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty. It refers to judicial, legislative and administrative competence. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application. These questions are generally a matter of conflict of laws, particularly private international law. So, where the contents of a web site are legal in one country and illegal in another. Inabsence of a uniform jurisdictional code, legal practitioners are generally left with conflict of law issues.

There is another major problem of cyber law. Because cyber law consider that internet has physical space. On the other hand it is belived that internet act as if it is a world itself. John Perry Barlow, has addressed the governments of the world and stated that "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract.

This governance will arise according to the conditions of our world, not yours. Our world is different." (Barlow, A Declaration of the Independence of Cyberspace).

The Declaration of Cybersecession states, "Human beings possess a mind, which they are absolutely free to inhabit with no legal constraints. Human civilization is developing its own collective mind. All we want is to be free to inhabit it with no legal constraints. Since you make sure we cannot harm you, you have no ethical right to intrude our lives. So stop intruding."

Lawrence Lessig's argument is that "The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once" (Lessing Code 190).

Cybersecession has little real impact on the Internet or the laws governing it. In practical terms, a user of the Internet is subject to the laws of the state or nation within which he/she goes online. So these suits are international in nature. In civil cases jurisdictional problems arises concerning the burden of proof.

B. Net Neutrality:

Net neutrality is another major area of interest. Generally it is considered that Internet activity should be neutral. It affects the regulation of the infrastructure of the Internet. Every packet of data sent and received by every user on the Internet passes through routers and transmission infrastructure. These are owned by a collection of private and public entities, including telecommunications companies, ISPs, universities, and governments. They are suggesting that the Internet is not independent. This is one of the most critical aspects of Cyber

Law. It has immediate jurisdictional implications. It is considerd that laws in force in one jurisdiction have the potential implication, but it may have another dramatic effects in other jurisdictions. As a result the host servers or telecommunications companies etc may be affected.

C. Free Speech in Cyberspace:

Cyberspace has torn down traditional barriers between individual's ability to publish in the traditional print media. Through an internet connection a person has the potential to reach an audience of millions with a little distribution costs. This new form of highly-accessible authorship in cyber space raises questions and legal complexities

relating to the freedom and regulation of speech in Cyberspace. These complexities have taken many forms.

Speech through cyberspace is new means of communication. It is known as Open Net Initiative. It is also regulated by the government of some countries. The mission of Open Net Initiative is to investigate and challenge the state filtration and surveillance practices in order to generate a credible picture of these practices. Filtration of internet-speech in various countries is a known fact.

China is the most rigorous in its attempts to filter unwanted parts of the internet from its citizens. Other countries including Singapore, Iran, Saudi Arabia, and Tunisia have engaged in similar practices. Chinese government for a short time transparently forwarded requests to the Google search engine to its own, state-controlled search engines. These examples of filtration bring to light many underlying questions concerning the freedom of speech. The government have a legitimate role in limiting access to information.

The recent blocking of blogspot and other websites in India failed to reconcile the conflicting interests of speech and expression on the one hand and legitimate government concerns on the other hand. In the UK the case of Keith-Smith v Williams confirmed that existing libel laws to internet discussion.

D. Internet Regulation in different Countries:

In some United States law that does restrict access to materials on the internet, but does not truly filter the internet. Many Asian and Middle East nations use to block material that their governments have deemed inappropriate for their citizens to view. China and Saudi Arabia are two excellent examples of nations that have achieved high degrees of success in regulating their citizens access to the internet.

16. Scope of Cyber law

Invention of computer, Internet, computer network, Information Technology (IT) and Information Communication Technology (ICT) changed the face of the world civilization. The world become very near to all. Every information is very much available to our door by the blessing of the technological revolution. Todays world may be called a networked world.

Cyber Law is the law governing computer and the Internet. Today's highly digitalized world, almost everyone is related with the cyber law.

Sky-Civilization influenced over the human society of the world tremendously through Information and communication Technology (ICT). The scope of the ICT is so vast and striking that almost all the people of the world is under one network. The life becomes comfortable and the whole world becomes under the grip of hand.

Cyber crimes are related with online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, email hijacking, denial of service, hacking, pornography, defamation etc are becoming common.

This present emerging contribution of the science should be regulated by law for the better interest of the human society and civilization. So the law related to control the behavior, rights, duties and obligations of the beneficiaries of Satellite Station, Satellite communication, internet, cyberspace, Information and Communication Technology (ICT) etc is termed as the subject of Cyber Law.

The Internet is a worldwide, publicly accessible network of interconnected computer networks. It consists of millions of smaller domestic, academic, business, and government networks. These together carry various informations and services, such as electronic mail, online chat, file transfer, and the interlinked Web pages and other documents of the World Wide Web (www).

The Internet does not tend to make geographical and jurisdictional boundaries. But Internet users are remaining under physical jurisdictions. For Example an internet user of Bangladesh conducting a transaction with another user in china through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial

limitations. There is no uniform, international jurisdictional law of universal application. These questions are generally a matter of conflict of laws, particularly private international law.

Another major problem of cyber law is that whether the Internet as if it has physical space or to act as if the Internet is a world itself. John

Perry Barlow, has addressed the governments of the world and stated that "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different." (Barlow, A Declaration of the Independence of Cyberspace).

The Declaration of Cybersecession states, "Human beings possess a mind, which they are absolutely free to inhabit with no legal constraints. Human civilization is developing its own collective mind. All we want is to be free to inhabit it with no legal constraints. Since you make sure we cannot harm you, you have no ethical right to intrude our lives. So stop intruding."

Lawrence Lessig's argument is that "The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once" (Lessing Code 190).

Internet structure has raised several judicial concerns. Internet is independent of any geographic location. Individuals connect to the Internet and interact with others. It is possible for them to withhold personal informations and make their real identities anonymous. The laws that could govern the Internet, would be fundamentally different from laws that geografic nations use today.

Allmost cyber crimes are conventional. So these crimes can be handled by the conventional laws of the states. But cybersapace, Intennet etc are beyond the territorial jurisdiction. But the person who uses the internet has a personal territorial jusisdiction. The local ICT they uses are also have an geographical identity.

The ICT is new concept. Allmost all the people of the world are now connected with ICT for their activities. So cyberlaw is a new concept. It is developing day by day. Different country enacted the new law related to cyberlaw.

So cyber law has a vast scope in near future. As much as cyberspace and ICT influenced the world, the need of the cyberlaw will be required. Cyber law is now concern with conventional law and also cyberspace law. But it has some barrier due to conflict with the conventional view point of law.

The concept of Cyber space and internet and computer network is a reality. The necessaty of the ICT cannot be denied. So barrier of the

cyber law will be realized and may be solved in due course. We are hopefull for the best. Concerning all these it can be conclude that Cyberlaw will open the door of a widest field of law. So cyber law has a great prospect in near future.

17. Utility of Cyber law:

Computers have become integral parts of the modern day homes and workplaces. Countries around the world continue to exhibit an encouraging trend of computer usage. Most academic institutions have invested in the best technology to keep their students equipped and informed.

As for the workplaces, there is a gradual trend towards a possible future brimming with 'paperless and shelf less offices'. The dependence on computers is increasing day by day. The better and faster machines are geared up to fulfill operations that were not even imagined a few years back.

The usage of computers have opened up newer possibilities for commerce and given fresh lease of life to several industries. The flexibility and economic feasibility of the Internet has transformed the cyberspace into a colossal market abundant with opportunities. The cyberspace knows no boundaries, no parameters and no boundary of a place as it connects people around the world. The cyber world has rendered our physical tangible world a much smaller place with distance and time being no longer compulsion of the modern day human.

Computers and their influence have traversed into almost every sector. Business, travel, education, entertainment or any other industry cannot comprehend progress without the help of these machines.

Students, professionals and organizations around the world need to understand the inescapable truth that computers are here to stay and in the definite future, it might be difficult to even move an inch without it having an effect on us.

Considering the present trend, it has become almost obligatory for everyone to understand the jurisprudence of Cyberlaw that countries worldwide have framed to regulate and control the use of computers. The inevitable addiction to technology, even though has revolutionized the society with the boons of mobility and flexibility. At the same time it has rendered us potential victims to a handful willing to exploit their knowledge and skills.

The alarming growth of cyber crimes is an issue. Nations are beginning to scrutinize in order to build better defense mechanisms. The biggest defense to technology crimes is creating widespread awareness among the various sections of society, who after all are the most vulnerable.

It is a common foolishness to isolate cyber crime as the only focus of cyber jurisprudence. In fact the study goes beyond into significant subjects like electronic commerce and cyber intellectual property rights. There are economic possibilities but scarcity of equipped professionals. The study of cyber laws hence can open doors to innumerable lucrative opportunities and can be seen as a viable next step to a successful career.

A new field of law i.e. Cyberlaw comes to society with various question and prospect. New civilization is technological civilization. It will be the Cyberspace nationality on the Networked world. Cyberlaw will govern this nationality.

18. Importance of cyber law:

Cyber Law is the law governing computers and the Internet. In today's highly digitalized world, almost everyone is affected by cyber law. For examples

1. Almost all transactions in shares are in demitting form. The increased use of online share trading transactions has led to a large number of frauds involving identity theft.
2. Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form. Criminals are targeting this data for espionage and extortion.
3. Government forms including income tax returns, company law forms etc are now filled in electronic form.
4. Consumers are increasingly using credit cards for online and offline shopping. This has led to a huge increase in the number and value of credit card frauds.
5. Most people are using email, cell phones and SMS messages for communication.
6. The extensive use of blogs and networking sites has led to cyber stalking and defamation cases.

7. Most banking transactions take place through electronic online.
8. Even in "non-cyber crime" cases, important evidence is found in computers, cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
9. Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, email hijacking, denial of service, hacking, pornography etc are becoming common.
10. Digital signatures and e-contracts are fast replacing conventional methods of transacting business.

Chapter–2

Cyber Jurisprudence & Human Rights

1. Jurisprudence of Cyber Law
2. Ethics of Cyber Jurisprudence
3. Importance of Cyber Jurisprudence
4. Origin of Cyber Law
5. Human rights and cyber Jurisprudence
6. Cyber Jurisprudence and Governance
7. Sources of Cyber law
8. What is Internet Citizen & Cyber Nationality?
9. What is Cyber Jurisdiction?

1. Jurisprudence of Cyber Law:

Jurisprudence is the branch of philosophy concerned with the law. It is a legal philosophy. So Jurisprudence of Cyberlaw is the philosophy concern with the Cyberlaw and also the conventional law that related with cyber crime.

The phenomenal growth of the Internet is unparallel. Internet has provided a new horizon in the economics, management, administration, globalization, transparency and interaction among human of the world. It has gripped popular imagination by providing easy communication, entertainment, leisure and education.

The global village or globalization is a reality today than it was ever before. The Internet is continually changing the dynamics of the world. A new law needs to this changed global society.

Roscoe Pound said, **"Legal order must be flexible as well as stable. Law must be overhauled continually and refitted continually to the change in social life which it is to govern."**

Indian Parliament legislate the Cyberlaw, The Information Technology Act 2000. Technology is ever changing and more so in the cyber world. Bangladesh also legislate the IT policy 2002 and approved Bangladesh Information technology Act. 'Cyberlaw - The Bangladesh Perspective' is a praiseworthy work on the statute.

Cyber jurisprudence is still in its initial stage. In this respect there are many questions but no answer till now. Duggal's book throws up

more questions than it answers. These questions should bring distinctly into the public domain then it will be a great service to cyber jurisprudence. Cyberlaws are grappling with a range of issues.

Conventional law is the law of the land that the jurisprudence deals in. Jurisprudence of Cyberlaw provides an extra-territorial jurisdiction in the prevailing circumstances of the networked world. Duggal's analyses the issue of jurisdiction from all angles. It is exciting and stimulating to the legal mind. In the changed situation the judiciary is tackling these problems.

Cyberlaw is pressing hard against the existing and settled boundaries of legal principles. It is an unforeseen circumstances and unique issues of law that the cyber world presents. The legislation is providing some guidelines on a broad framework to the judiciary.

Cyber Jurisprudence is a new legal philosophical concept. It is developing based on information technology and networked world. New problem arises on emergent growing of technological issues based on cyber culture and civilization. The future war and peace, humanity and morality, life and enjoyment, society and individuality are almost going to cyber space. To make all this things under legal framework is a vast philosophical aspect. So cyber jurisprudence is the philosophy of cyberworld, legal relation with the mankind.

2. Ethics of Cyber Jurisprudence:

Ethics is the motivation based on ideas of right and wrong. It is the philosophical study of moral values and rules of mankind and the principles of right and wrong that are accepted by an individual or a social group.

Ethics and morality differs in different circumstances. In general each and everything which is opposed to public policy, against public welfare and which may disturb public tranquility may be termed to be immoral and unethical. Every person might be in two frames of minds. The opinion of every person may be quite diversified as well as ambiguous. The issue of 'cyber-ethics' is full of ambiguity. Today in the present era it is needed to evolve a cyber-jurisprudence.

The right to freedom of belief, thought and expression which are basic principals envisaged in constitution. The freedom of press is also a guaranteed right provided by the constitution. Further the constitution also guarantees right to information. The citizens have the

fundamental right to know what is happening around them. The constitution guarantees the right to privacy. Supreme Court of Bangladesh is the guardian of fundamental rights as confirmed by the constitution. Every man has some penumbral zones of privacy. These cannot be infringed upon even by the State.

As a matter of principal there is no doubt that a conflicts between a personal-interest and national-interest undoubtedly the national-interest should prevail. Further there is a dire need for evolving a code of Ethics on the Cyberspace and discipline.

So ethics of cyber jurisprudence is a new concept based on information technology, cyberspace, cyber world, internet nationality etc.

3. Importance of Cyber Jurisprudence:

Computer, Internet, Networks, Cyberspace and Cyberlaw has opened a new horizon of the civilization. Information Technology (IT) and Information and Communication Technology (ICT) have given a new dimension of the civilization. This may be termed as E-civilization. The E-civilization developed upon the cyberspace of networked world. This civilization made a revolution upon nationality, sovereignty and legal structure.

The emergence of cyber jurisprudence around the world has prompted the growth of newer dimensions in career choices. Students and professionals willing to understand this unique and growing field of study have opened doors to opportunities worldwide.

It is a common misconception that Cyber Laws is a field of study only for legal professionals. Education on Cyberlaws in fact equips professionals from diverse backgrounds about the various compliance issues. It is need to address in any environment which relies on information technology. This multi-dimensional attribute of Cyber Jurisprudence has made training mandatory for professionals in Law, IT, Engineering, Banking, Insurance, Business, Outsourcing, Government, Police and other sectors. So cyber jurisprudence awareness is essential in traditional employee orientation programs globally.

Cyberlaws is gradually evolving into a separate discipline. It is creating lucrative prospects for student of Cyberlaws. A dedicated training on technology based jurisprudence is essential.

The world is constantly seeking experts or analysts of cyber crimes. Consultants, lawyers and academics in the field of cyber law are also

required. The opportunities for professionals equipping themselves with this new field are numerous. Consultants of Cyberlaws can help against cyber threats. They can also help the petitioners against online scammers and fraudsters. Academicians can conduct lectures, workshops and seminars. Trained individuals could help draft rules and regulations in order to govern the cyberspace.

There is a distinct global shortage of Cyberlaw experts. Students and professionals can be trained up on this growing field. Training Programs and Courses may play a vital role in this embryonic stage of Cyberlaws Education and plans. It can meet the growing global need for skilled workforce. Student can find relevant jobs in their respective fields. Various jobs also help them to build up their Resumes successfully. So they can highlight their merits to the fullest, thereby enabling students to come closer to landing their dream jobs.

4. Origin of Cyberlaws

Cyberspace is the metaphorical space of computer systems and networks. Here electronic data are stored and online communication takes place. The term originates in science fiction. It includes various kinds of virtual reality of the computer users.

Internet structure has raised several judicial concerns. Internet is independent of any geographic location. Individuals connect to the Internet and interact with others. It is possible for them to withhold personal informations and make their real identities anonymous. The laws that could govern the Internet, would be fundamentally different from laws that geografic nations use today.

Internet governs itself. It is not obeying the laws of a particular country. Internet citizens will obey the laws of electronic entities like service providers. Instead of identifying as a physical person, Internet citizens will be known by their usernames or email addresses. Since the Internet defies geographical boundaries, national laws will no longer apply. An entirely new set of laws will be created to address concerns like intellectual property and individual rights. In effect, the Internet will exist as its own sovereign nation.

In some United States law restrict access to materials on the internet. But they do not truly filter the internet. Many Asian and Middle East nations use to block material that their governments have deemed inappropriate for their citizens to view. China and Saudi Arabia are two

excellent examples of nations that have achieved high degrees of success in regulating their citizens access to the internet. Moreover Internet faced several Internet crime like E-mail crime, E-mail terorism, E-mail abuse, Passward frud, Hacking, Torajan, Virus and worm, economic crime, phornography etc.

Internet should be regulated. Substantial regulation, both public and private, by many parties and at many different levels should be provided. In different countries there are regulating laws. Bangladesh is following laws mentioned below:

1. ICT Policy in Bangladesh
2. Bangladesh Information and Technology Act (Proposed)
3. The (Indian) Information Technology Act 2000
4. UNCITRAL Model Law on Economic Commerce
5. Conventional laws like penal code,
6. Criminal procedure code,
7. Civil procedure code,
8. Law of contract
9. Law of evidence etc.

The Internet has revolutionary impact on the computer and communications of the World. The invention of the telegraph, telephone, radio, and computer set the platform for the unprecedented integration of capabilities. It is a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

Beginning with the early research in packet switching this exciting new technology developed tremendously and involves many aspects like technological, organizational, and community. Its influence reaches not only to the technical fields of computer communications but throughout the global society. The global society is using the online tools to accomplish electronic commerce, information acquisition, and community. The Internet today is a widespread information infrastructure for the civilization.

So to regulate the physical nature of the emergent technology, cyber space, internet citizen, cyber world with relation of mankind, cyber law is developing. As the crimes are mostly conventional the Cyberlaw is developing day by day with the combination of conventional law. Different countries are enacted Law on the various issues of cyber crime. The investigation process has also developed. But all these are

the combination of conventional laws and new laws. This cyber law is in primitive stage. Days are coming that this law will come into existence as a new branch of law.

5. Human rights and cyber Jurisprudence:

Man is a living being like other animel. But their knowledge, nature, responsibility and freedom of willpower make them different from other animls. As a human being, from the very beginning of their race in earth, posseses several rights, duties and responsibilities towords others. It is the basic right or freedom to which all human beings are entitled and in their exercise, a government may not interfere. These are the rights to life and liberty, as well as freedom of thought and expression and equality before the law etc.

These rights that man require from his birth, to maintain his legal life as a man, is called human rights. Now a days, human rights are the universal rights of human beings regardless of jurisdiction or other factors, such as nationality, ethnicity, or religion. The idea of human rights descended from the philosophical idea of natural rights. The United Nations Universal Declaration of Human Rights are conceptualized as a inherent human dignity to retain their universal character.

The existence, validity and the content of human rights continue to be the subject to debate in philosophy, political science and many other forms. Legally, human rights are defined in international law and covenants in the domestic laws of many states. The doctrine of human rights goes beyond law and forms a fundamental moral basis for regulating the contemporary geo-political order as a democratic ideals.

The human rights and cyberlaw should exsist side by side. Cocerning cyberspace, Internet, Global net nationality, cyber crime etc are the subject matter of human right. The violation of human right by net natioanl should be taken into account. In this respect cyber jurisprudence has the positive role for the management of cyber law for the interest to protect the rights of global nations and net-nations.

6. Cyber Jurisprudence and Governance

Internet structure has raised several judicial concerns. Internet is independent of any geographic location. Individuals connect to the Internet and interact with others. It is possible for them to withhold personal informations and make their real identities anonymous. The

laws that could govern the Internet, would be fundamentally different from laws that geografic nations use today.

David Johnson and David Post offer a solution to the problem of Internet governance. They stated that, "It becomes necessary for the Internet to govern itself. Instead of obeying the laws of a particular country, Internet citizens will obey the laws of electronic entities like service providers. Instead of identifying as a physical person, Interne citizens will be known by their usernames or email addresses. Since the Internet defies geographical boundaries, national laws will no longe apply. Instead, an entirely new set of laws will be created to address concerns like intellectual property and individual rights. In effect, the Internet will exist as its own sovereign nation."

Internet should be regulated. Substantial regulation, both public and private, by many parties and at many different levels should be provided. There are four primary modes of regulation of the internet described by Lawrence Lessig in his book, Code and other laws of Cyberspace. These are given below :

1. "Law: Standard East Coast Code, and the most self-evident of the four modes of regulation. As the numerous statutes, evolving case law and precedents make clear, many actions on the internet are already subject to conventional legislation (both with regard to transactions conducted on the internet and images posted). Areas like gambling, child pornography, and fraud are regulated in very similar ways online as off-line. While one of the most controversial and unclear areas of evolving laws is the determination of what forum has subject matter jurisdiction over activity conducted on the internet, particularly as cross border transactions affect local jurisdictions, it is certainly clear that substantial portions of internet activity are subject to traditional regulation, and that conduct that is unlawful off-line is presumptively unlawful online, and subject to similar laws and regulations. Scandals with major corporations led to US legislation rethinking corporate governance regulations such as Sarbance-Oxley Act."

2. "Architecture: West Coast Code: these mechanisms concern the parameters of how information can and cannot be transmitted across the internet. Everything from internet filtering software (which searches for keywords or specific URLs and blocks them before they can even appear on the computer requesting them), to encryption programs, to the very basic architecture of TCP/IP

protocol, falls within this category of regulation. It is arguable that all other modes of regulation either rely on, or are significantly supported by, regulation via West coast Code."

3. "Norms: As in all other modes of social interaction, conduct is regulated by social norms and conventions in significant ways. While certain activities or kinds of conduct online may not be specifically prohibited by the code architecture of the internet, or expressly prohibited by applicable law, nevertheless these activities or conduct will be invisibly regulated by the inherent standards of the community, in this case the internet "users." And just as certain patterns of conduct will cause an individual to be ostracized from our real world society, so too certain actions will be censored or self-regulated by the norms of whatever community one chooses to associate with on the Internet."

4. "Markets: Closely allied with regulation by virtue of social norms, markets also regulate certain patterns of conduct on the internet. While economic markets will have limited influence over non-commercial portions of the internet, the internet also creates a virtual marketplace for information, and such information affects everything from the comparative valuation of services to the traditional valuation of stocks. In addition, the increase in popularity of the internet as a means for transacting all forms of commercial activity, and as a forum for advertisement, has brought the laws of supply and demand in cyberspace."

7. Sources of Cyber law:

Cyber law is a new branch of law. The frame work not yet sufficiently developed. It is developing day by day. The information technology unthinkably spread over the whole global society and civilization. It influenced all the nations of the world. But accordingly the structure of laws was not yet framed on regular basis. Still many countries are enacting their laws on information technology. Cyber laws are framing on the basis of some sources. These are as follows.

1. Convention laws those are followed by the global states.
2. Cyber law books,
3. International contacts and agreements,
4. Statutory laws passed by the parliament of different country.
5. International conventions, etc.

8. What is Internet Citizen & Cyber Nationality?

Internet has a global network. Every individual using internet has an identity. They are known by their users name and email address. So they will be known as Internet Nation or Cyber citizen. It is considered that Internet is independent of any geographical location. Individuals connect to the internet and interact with each other. It is possible for them to withhold personal information's. The can make their identity anonymous. So the cyber nationality would be different from the geographical nation of today.

David Johnson and David Post offer a solution to the problem of Internet governance. They stated that, "It becomes necessary for the Internet to govern itself. Instead of obeying the laws of a particular country. Internet citizens will obey the laws of electronic entities like service providers. Instead of identifying as a physical person, Internet citizens will be known by their usernames or email addresses. Since the Internet defies geographical boundaries, national laws will no longer apply."

Inspite of all this possiblities, internat citizen is a citizen of perticular country. As a person an internet user must obey the law of the country. Moreover the internet service provider, the IT infrastructure also controlled by the country where it is located. So it is most defficult to have sovern identity of an Internet citizen or cyber nationality.

9. What is Cyber Jurisdiction?

The Internet does not tend to make geographical and jurisdictional boundaries. But Internet users are remaining under physical jurisdictions. These are

1. The laws of the state in which the user resides,

2. The laws of the state that apply where the server hosting the transaction is located, and

3. The laws of the state which apply to the person or business with whom the transaction takes place.

So a single transaction may involve the laws of at least three jurisdictions. For Example a internet user of Bangladesh conducting a transaction with another user in china through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty. It refers to judicial, legislative and administrative competence. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application. These questions are generally a matter of conflict of laws, particularly private international law. So, where the contents of a web site are legal in one country and illegal in another. In absence of a uniform jurisdictional code, legal practitioners are generally left with conflict of law issues.

There is another major problem of cyber law. Because cyber law consider that internet has physical space. On the other hand it is belived that internet act as if it is a world itself. John Perry Barlow, has addressed the governments of the world and stated that, "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different." (Barlow, A Declaration of the Independence of Cyberspace).

The Declaration of Cybersecession states, "Human beings possess a mind, which they are absolutely free to inhabit with no legal constraints. Human civilization is developing its own collective mind. All we want is to be free to inhabit it with no legal constraints. Since you make sure we cannot harm you, you have no ethical right to intrude our lives. So stop intruding."

Lawrence Lessig's argument is that "The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once" (Lessing Code 190).

Cybersecession has little real impact on the Internet or the laws governing it. In practical terms, a user of the Internet is subject to the laws of the state or nation within which he or she goes online. So these suits are international in nature. In civil cases jurisdictional problems arises concerning the burden of proof.

Chapter–3
Internet and Networks

1. **What is Computer Networks or Network**
2. **Definition of Computer Network**
3. **What are the Components of computer networks?**
   a. **Computers**
   b. **Workstations**
   c. **Servers**
   d. **Classification of computer networks**
4. **Definition of Internet**
5. **Internet and its service**

1. What is Computer Networks or Networks?

Network means computer network. Network of computers is the interconnection of two or more computers together using some form of communications medium. It constitutes some specific purposes. A computer connected to a non-computing device, (for example networked to a printer via an Ethernet link) may also represent a computer network. Same basic functions are generally present in this case as with larger numbers of connected computers.

2. Definition of Computer Network:

According to Wikipedia, the free encyclopedia,

"A computer network is multiple computers connected together using a telecommunication system for the purpose of communicating and sharing resources."

Glossary of Telecommunication Terms states that

"A computer network is a network of data processing nodes that are interconnected for the purpose of data communication", the term "network" being defined as "An interconnection of three or more communicating entities".

3. What are the Components of computer networks?

In a computer network some basic components are used. Brief descriptions about the components are given below

a. Computers: The basic components of an average network are individual computers. These are used as either workstations or servers (including personal computers).

b. Workstations: There are many types of workstations. These may be incorporated into a particular network. The workstations have

1. High-end displays,
2. Multiple CPUs,
3. Large amounts of RAM,
4. Large amounts of hard drive storage space, or other enhancements required for special data processing tasks,
5. Graphics or other resource intensive applications

Many networks use thin clients instead of workstations either for data entry and display purposes or in some cases where the application runs entirely on the server.

c. Servers: Server is of several types. Some common types of servers and their purpose are given below.

1. File server: File server stores various types of files and distributes them to other clients on the network.

2. Print server: Print server controls and manages one or more printers and accepts print jobs from other network clients. These servers are for spooling the print jobs, and performing most or all of the other functions that a workstation would perform. These servers accomplish a printing task if the printer is connected directly to the workstation's printer port.

3. Mail server: Mail Servers are generally SMTP, IMAP, and Post Office Protocol. These servers' stores, sends, receive, routes, and perform other email related operations for other clients on the network.

4. Fax server: Fax server stores, sends, receives, routes, and performs other functions necessary for the proper transmission, reception, and distribution of faxes.

5. Telephony server: Telephony server is H.323, MGCP, SCCP, and SIP. These server Performs telephony related functions such as answering calls automatically, performing the functions of an interactive voice response system, storing and serving voice mail,

routing calls between the Public Switched Telephone Network (PSTN) and the network or the Internet (e.g., voice over IP (VoIP) gateway).

6. Proxy server: Proxy server performs some type of function on behalf of other clients on the network to increase the performance of certain operations or as a security precaution to isolate network clients from external threats.

7. Remote Access Server (RAS): Remote Access Server (RAS) monitors modem lines or other network communications channels for requests to connect to the network from a remote location, answers the incoming telephone call or acknowledges the network request, and Performs the necessary security checks and other procedures are necessary to log a user onto the network.

8. Application server: Application server performs the data processing or business logic portion of a client application. It accepts instructions for operations to perform from a workstation and serving the results back to the workstation. The workstation performs the user interface or GUI portion of the processing (i.e., the presentation logic) that is required for the application to work properly, for example Jetty, Tomcat, BEA-WebLogic.

9. Game server: Game server dedicated computer system running game hosting software.

10. Web server: Web server stores HTML documents, images, text files, scripts, and other Web related data (collectively known as content), and distributes this content to other clients on the network on request.

11. Database server: Database server used for the storage of all data.

12. Backup server: Backup server has network backup software installed and has large amounts of hard drive storage or other forms of storage (tape, etc.) available to it to be used for the purpose of ensuring that data loss does not occur in the network.

d. Classification of computer networks

1. Personal Area Network (PAN):
2. Local Area Network (LAN):

3. Campus Area Network (CAN):

4. Metropolitan Area Network (MAN):

5. Wide Area Networks (WAN):

1. Personal Area Network (PAN): A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The devices may or may not belong to the person in question. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). Personal area networks may be wired with computer buses such as USB and FireWire. A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth.

2. Local Area Network (LAN): Local Area Network (LAN) is limited to a relatively small spatial area such as a room, a single building, a ship, or an aircraft. Local area networks are sometimes called a single location network. For administrative purposes, large LANs are generally divided into smaller logical segments called workgroups. A workgroup is a group of computers that share a common set of resources within a LAN.

3. Campus Area Network (CAN): Campus Area Network (CAN) that connects two or more LANs but that is limited to a specific (possibly private) geographical area such as a college campus, industrial complex, or a military base. A CAN is generally limited to an area that is smaller than a Metropolitan Area Network.

4. Metropolitan Area Network (MAN): Metropolitan Area Network (MAN) that connects two or more Local Area Networks or CANs together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area. Multiple routers, switches & hubs are connected to create a MAN

5. Wide Area Networks (WAN): Wide Area Networks (WAN) is a data communications network that covers a relatively broad geographic area and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model; i.e.

4. Definition of Internet:

Definition of Internet was developed in consultation with members of the internet and intellectual property rights communities. The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term "Internet". Internet refers to the global information system that

(i) Internet is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

(ii) Internet is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) Internet provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure **described herein.**

5. Internet and its services:

The Internet has changed much in the two decades since it came into existence. It was conceived in the era of time-sharing, but has survived into the era of personal computers, client-server and peer-to-peer computing, and the network computer.

The Internet is a creature of the computer, not the traditional network of the telephone or television industry. It must, continue to change and evolve at the speed of the computer industry. It is now changing to provide such new services as real time transport, in order to support audio and video streams.

The evolution will bring new applications - Internet telephone and Internet television. It is evolving to permit more sophisticated forms of pricing and cost recovery. It accommodates another generation of underlying network technologies with different characteristics and requirements from broadband residential access to satellites.

The debates over control of the domain name space and the form of the next generation IP addresses, a struggle to find the next social structure that will guide the Internet in the future.

Chapter–4
Cyber Crime

1. What is Cyber Crime
2. Definition of Cyber crime
3. Types of Cyber Crimes
   1. Financial crimes
   2. Cyber Pornography
   3. Sale of Illegal Articles
   4. Online Gambling
   5. Intellectual Property Crimes
   6. Email Spoofing
   7. Forgery
   8. Cyber Defamation
   9. Cyber stalking
4. Technical Cyber Crimes
   a. Unauthorized Access
   b. Theft of Information Contained in Electronic Form
   c. Email bombing
   d. Data diddling
   e. Salami attacks
   f. Denial of Service attack
   g. Virus attacks
   h. Worms Attacks
   i. Logic bombs
   j. Trojan attacks
   k. Internet time theft
   l. Web Jacking
   m. Theft of computer system
   n. Physically damaging a computer system

---

1. What is Cyber Crime:

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced a special type of loom. This device allowed the repetition of a series

of steps in the weaving of special fabrics. At this Jacquard's employees became fear that their traditional employment and livelihood was being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.

The abacus was the earliest form of a computer that has been used since 3500 B.C. in India, Japan and China. The era of modern computers has begun with the analytical engine of Charles Babbage.

Today, computers have come a long way. The neural networks and nano-computing are promising to turn every atom in a glass of water. Now a computer is capable of performing a billion operations per second.

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age everything from microwave ovens and refrigerators to nuclear power plants is being run on computers. So cyber crime has assumed sinister implications on the computer world and the human society.

2. Definition of Cyber crime:

Cyber crime may be defined as E-crime. E-crime covers offences where a computer or other Information and Communication Technology are used to commit an offence. The actual offence committed may be a traditional offence. These are theft , fraud , identity crimes, harassment, threatening violence, possessing, making, or distributing objectionable material, e.g. child pornography, criminal breach of copyright

E-crime is a type of offence specifically related to computers. Hacking, unauthorized access to a computer system, distributing an electronic virus designed to damage or accesses a computer system, distributing software for the commission of a crime, launching a denial of service attack intentionally or causing a computer system to deny service to any authorised user.

So we defined it as, **"E-crimes are almost conventional crimes in nature committed by using Computer & ICT with an intention to make social disorder."**

3. Types of Cyber Crimes:

The followings are the cyber crime:

1. Financial crimes
2. Cyber Pornography
3. Sale of Illegal Articles

4. Online Gambling
5. Intellectual Property Crimes
6. Email Spoofing
7. Forgery
8. Cyber Defamation
9. Cyber stalking

Cyber Crime can be differentiating from Conventional Crime. Cyber crime can involve criminal activities that are traditional in nature. These are theft, fraud, forgery, defamation, mischief etc and subject matter of the Penal Code. The abuse of computers has also given birth to new crimes that are addressed by The (Indian) Information Technology Act, 2000 and Bangladesh Information Technology Act (Proposed).

Cyber crimes may be defined as acts those are punishable by Bangladesh Information and Technology Act (Proposed) and the (Indian) Information Technology Act 2000. Cyber crime is the unlawful acts wherein the computer and Information Communication Technology are used either a tool or a target or both. Cyber Crime covers many crimes. The computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers.

1. Financial crimes: Financial crimes include cheating, credit card frauds, money laundering etc. For example, Punjab National Bank was cheated to the tune of Rs. 1.39 crors through false debits and credits in computerized accounts. In another case, Rs. 2.5 lacs were misappropriated from Bank of Baroda through falsification of computerized bank accounts. Computer operator can use the details of credit cards if he knows, to make online purchases on various websites.

2. Cyber Pornography: Cyber Pornography includes pornographic websites; publish and print pornographic magazines by using computers and the Internet to download and transmit pornographic pictures, photos; writings etc. "Air Force Balbharati School case" is one of the pornographic case references.

3. Sale of Illegal Articles: Sale of illegal articles include sale of narcotics, weapons and wildlife, illegal medicine etc. This can be by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Many of the auction sites are believed to be selling cocaine in the name of honey. In Bangladesh it is also practicing.

4. Online Gambling: Many websites offer online gambling. Many of these websites may actually be fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported. These sites may have any relationship with drug trafficking. This is yet to be explored.

5. Intellectual Property Crimes: Intellectual Property Crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. Some cyber squatters are registering domain with Network solutions under different fictitious names. Transfer of domain names to any third party should be restricted.

6. Email Spoofing: A spoofed E-mail is that E-mail which appears to originate from one source but actually has been sent from another source. As for example Babar has an E-mail address Babar@bahar.com. His enemy, Karim spoofs his E-mail and sends obscene messages to all his friends. Since the E-mails appear to have originated from Babar, his friends could take offence. The relationships may be spoiled for ever.

A teenager made millions of dollars by spreading false information about certain companies whose shares had short sold. This misinformation was spread by sending spoofed E-mails, purportedly from news agencies like Reuters. The share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels. As a result thousands of investors lost a lot of money. This was an American case.

Once numerous customers of a bank decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating

The bank was in very bad shape financially. It could close operations at any time. The spoofed email appeared to have originated from the bank itself.

7. Forgery: Counterfeit currency notes, postage and revenue stamps, mark sheets, certificate etc can be forged using sophisticated computers, printers and scanners. These are made using computers, and high quality scanners and printers. This is becoming a booming business now days.

8. Cyber Defamation: This occurs when defamation takes place with the help of computers or the Internet. For example someone publishes defamatory matter about someone on a website or sends E-mails to his friends containing defamatory information.

Cyber defamation first case of India was reported when a company's employee started sending derogatory, defamatory and obscene E-mails about its Managing Director. The E-mails were anonymous and frequent. Those were sent to many of their business associates to tarnish the image and goodwill of the company. The company was able to identify the employee with the help of a private computer expert. It was moved to Delhi High Court. The court granted an ad-interim injunction. The employee was restrained from sending, publishing and transmitting e-mails, which were defamatory or derogatory to the plaintiffs.

9. Cyber stalking: The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves a person's movements across the Internet. The person sends the messages on the bulletin boards frequently to the victim. He can enter into the chat-rooms and disturbed the victim by constantly sending emails.

4. Technical Cyber crimes:

There is another kind of Cyber crime that is called technical cyber crime. These are classified as follows.

a. Unauthorized Access
b. Theft of Information Contained in Electronic Form
c. Email bombing
d. Data diddling
e. Salami attacks
f. Denial of Service attack
g. Virus attacks
h. Worms Attacks
i. Logic bombs
j. Trojan attacks
k. Internet time theft
l. Web Jacking
m. Theft of computer system
n. Physically damaging a computer system

a. Unauthorized Access: Some body can access into the computer Systems or Networks activity for which he is not authorized to do so. This is commonly known as hacking. As per Bangladesh and Indian law, unauthorized access does occur, if hacking has taken place.

b. Theft of Information Contained in Electronic Form: Theft of Information is a kind of cyber crime. By this crime some body access into the computer Systems or Networks activity of another person. Then he collects information stored in computer hard disks and removed these information's. This is called theft of information contained in electronic form.

c. Email bombing: Email bombing occurs when a large number of emails send to the victim's computer. As a consequence the victim's email account or mail servers' might crash. For example a foreigner who had been residing in India for almost thirty years. He wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board. He kept sending e-mails till their servers crashed. This is called Email bombing.

d. Data diddling: Data diddling is a kind of cyber crime. By this activity it alters the raw data just before it processed by a computer. The NDMC Electricity Billing Fraud Case 1996 is an example. The computer network was used for receipt and accounting of electricity bills. Collection of money, computerized accounting, record maintenance and remittance in this bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

e. Salami attacks: Salami attack is one kind of financial crime. Here the computer program is altered. The alteration is so insignificant that in a single case it remains completely unnoticed. For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say 10 cents per month) from the account of every customer. No account holder will probably notice this unauthorized debit. The bank employee can illegally make a considerable amount of money per month.

A bank employee in USA was dismissed from his job. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault.

It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizeable

amount of money being transferred into his account every Saturday. Being an honest person, he reported the mistake to the bank authorities and the entire scheme was revealed.

f. Denial of Service attack: Denial of Service attack is one kind of cyber crime. The computer resource received so many requests which it can not handle. This crashes the computer resource. As a result the computer resource denies giving proper service to the authorized users. Another kind of denial of service attack is known as Distributed Denial of Service (DDoS) attack. Here the perpetrators are many. They are geographically widespread.

It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer. The victim's servers can not support the excess demands. This makes the server crash.

g. Virus attacks: Virus attacks are another kind of cyber crime. Viruses are one kind of programs that attach themselves to a computer or a computer file. Then they circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. In May 2000, a deadly virus became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion.

h. Worms Attacks: Worms attack is one kinds of cyber crime. Worms are unlike viruses. It does not need the host to attach them. They make functional copies of themselves. They do this repeatedly till they eat up all the available space on a computer's memory. Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. This worm affected thousands of computers. A team of experts worked almost three days to get rid of the worm. In the meantime many of the computers were disconnected from the network.

i. Logic bombs: Logic bombs are event dependent programs. These programs are created to do something only when a certain event occurs. Some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

j. Trojan attacks: Trojans is a kind of cyber crime. It is an unauthorized program which functions from inside of a computer. It is concealing what it is actually doing. There are many simple ways of installing a Trojan in someone's computer.

Here is an example. Two friends R and M had a heated argument over one girl B whom they both liked. When the girl is asked to choose, she chooses M over R. R decided to get even. On the 14th of February, he sent to M a Spoofed E-card, appeared to have come from B's mail account. The E-card actually contained a Trojan. As soon as M opened the card, the Trojan was installed on his computer. R now had complete control over M's computer and proceeded to harass him thoroughly.

k. Internet time theft: Internet time theft is a kind of cyber crime. Here an unauthorized person uses Internet hours but payment made by another person. It is a theft of Internet hours by using login name and password from various places causing wrongful loss of internet hours of other users. The Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the password of an Internet user. He accessed the computer and stole 107 hours of Internet time from the other person's account. He was booked for the crime by a Delhi court during May 2000.

l. Web Jacking: Web Jacking is another kind of cyber crime. It occurs when someone forcefully takes control of a website by cracking the password. After that he changes it. The actual owner of the website does not have any more control over his website. He does not know what appears on that website.

For example there is a recent incident in USA. The owner of a hobby website for children received an E-mail. This E-mail informed her that a group of hackers took control over her Website. They demanded 1 million dollars from her. The owner was a school teacher. She did not take the threat seriously and ignored the E-mail. After three days she received many telephone calls from all over the country that the hackers had web jacked her website. The hackers had altered a portion of the website 'How to have fun with goldfish'. In all the places of the website they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions. They bought piranhas from pet shops, tried to play with piranhas and were very seriously injured.

m. Theft of computer system is a kind of offence involves the theft of a computer, some parts of a computer or a peripheral attached to the computer.

n. Physically damaging a computer system is a crime that committed by physically damaging a computer and its peripherals.

Chapter–5

Tools and Techniques of Cyber Crime

1. Unauthorized Access
2. Packet Sniffing
3. Tempest attack
4. Password cracking
5. Buffer overflow
6. Trojans
7. Viruses
8. Worms

The cyber criminal while committing the cyber crime used some tools and techniques. This is very impotent and one should know these. The followings are the Tools and Techniques of Cyber Crime using by the cyber criminals. Brief descriptions are given below:

1. Unauthorized Access:

The word Access is defined in Section 2(1) (a) of the (Indian) Information Technology Act 2000 as **"gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network".**

According to Bangladesh Information Technology Act (Proposed) Access is defined in Section 3 (a) as, **"access" means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network."**

So, unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Thus are-

1. Access to a server by cracking its password authentication system is unauthorized access.

2. Switching on a computer system without the permission of the person in charge of such a computer system is also unauthorized access.

3. Access to Packet sniffing is a kind of unauthorized access.
4. Tempest attack is another kind of unauthorized access.
5. Password cracking is one kind of unauthorized access.
6. Buffer overflow is also a kind of unauthorized access.

2. Packet Sniffing:

Packet Sniffing is a technology used by crackers and forensics experts. For this data transmission is to be understood. It is known that data travels in the form of packets on networks. These packets are of various sizes depending on the network bandwidth. The amount of data is being carried in the packet in the measure of bytes. Each packet has an identification label also called a header. The header carries information of the source, destination, protocol, size of packet, total number of packets in sequence and the unique number of the packet.

The data carried by the packet is in an encrypted format for the sake of security and convenience in transmitting the data. This is also known as the hex of the data. The network layer is responsible for preparing the packet for transmission. This is the level where most hackers attack.

When a hacker wishes to intercept the transmission, would have to intercept the data packets. For doing this he would normally use a technology called Packet Sniffing. By using this technology a hacker is able to intercept all or some of the packets leaving from the victim (sender) computer. To use the sniffing technology the hacker needs to know the IP address of either of the parties involved in the communication. All packets leaving the IP address will be 'sniffed' by the Sniffer. All the data will be reported to the hakers in the form of logs. The sniffed data would still be in the hex format. Most Sniffers nowadays provide the facility of conversion of the stolen hex into actual human readable data. The detection of most packet Sniffers is impossible.

The Sniffer attaches itself to the network devices like the modem or the Network Interface Card (NIC). It is used by the victim computer to send and receive data. There are many commercially and conventionally available packet Sniffers today. Some can freely be downloaded from Internet. Some of the more famous Sniffers are ADMsniff-v08, AntiSniff-101, anti_sniff_researchv1-1-2, sniff, ethereal and Spynet.

3. Tempest attack:

Transient Electro-Magnetic Pulse Emanation Standard is TEMPEST. Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct the data. This allows remote monitoring of network cables or remotely viewing monitors. There are some fonts that remove the high-frequency information. An appropriately equipped car can park near the target premises can remotely pick up all the keystrokes and messages displayed on the computer monitor. This would compromise all the passwords, messages, and so on. By properly shielding computer equipment and network cabling the TEMPEST attack can be saved.

4. Password cracking:

A password is one kind of authentication. It is a secret word that a user must know in order to gain access. Computer password information is constantly being checked. To crack a password means to decrypt a password, or to bypass a protection scheme. The crack program is a useful tool for system administrators. By running the program on their own systems, they can quickly find users who use weak passwords. In other words, it is a policy enforcement tool. Password crackers are using utilities to guess passwords. Brutus is a popular password cracking utility. Brutus has both dictionary attack as well as a brute force attack capabilities.

5. Buffer overflow:

Buffer overflow is the most common way of breaking into a computer. The hackers insert excessive data in the input of a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input. This inserted executable code enables the hacker to break into the computer.

6. Trojans (for details See Chapter – 14):

In the 12th century BC, Greece declared war on the city of Troy. The dispute erupted when the prince of Troy abducted the queen of Sparta. He wanted to make her his wife. This naturally angered the Greeks and especially the queen of Sparta. The Greeks besieged Troy for 10 years but met with no success as Troy was very well fortified. In

a last effort, the Greek army pretended to be retreating, and left behind a huge wooden horse. The people of Troy saw the horse. They thought that it was some kind of present from the Greeks. They pulled the horse into their city. They did not know that the hollow wooden horse had some of the best Greek soldiers sitting inside it. At night the soldiers came out and opened the gates of the city. These soldiers along with the other Greeks soldiers fought together and killed the entire army of Troy. Similar to the wooden horse, a Trojan horse program pretends to do one thing while actually doing something completely different. Types of Trojans are -

a. Remote Administration Trojans (RATs)

b. Password Trojans

c. Privileges-Elevating Trojans

d. Key loggers

e. Destructive Trojans

f. Joke Programs

Some common Trojans

a. Back Orifice (BO)

b. NetBus

c. NetBus 2 Pro

d. Deep throat v 2

7. Viruses (for details See Chapter – 12)

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it. A virus program does not perform outright damage, delete or corrupt files of a computer. The virus program tries to hide its malicious function and tries to spread onto as many computers as possible very quickly. Viruses can be very dangerous. A virus that can stops a computer and displays a wrong message. This virus may be fatal in case of hospital life-support computer. Generally, there are two main classes of viruses.

1. The file infector viruses: These viruses attach themselves to ordinary program files. The file infectors are again two types;

a. Direct action virus: A direct-action virus selects one or more other programs to infect and the program that contains it is executed. The Vienna virus is an example of a direct-action virus.

b. Resident virus: A resident virus hides itself somewhere in memory. At the first time an executed program is infected. Thereafter it infects other programs when they are executed or when certain other conditions are fulfilled. Most of the viruses are resident except the Vienna virus

2. The Boot-record infectors: These viruses infect executable code found in certain system areas on a disk, which are not ordinary files. Such viruses are always resident viruses. A few viruses (Tequila virus) are able to infect both. These are often called "multi-partite" viruses; another name is "boot-and-file" virus. File system or cluster viruses are those that modify directory table entries so that the virus is loaded and executed before the desired program.

Note that the program itself is not physically altered. Only the directory entry is altered. Some consider these infectors to be a third category of viruses, while others consider them to be a sub-category of the file infectors. These are –

a. Stealth virus

b. Polymorphic virus

c. Fast and slow infectors

d. Sparse infector

e. Companion virus

f. Armored virus

g. Virus hoax

8. Worms:

A computer worm is a self-contained program or set of programs that is able to spread functional copies of itself or its segments to other computer systems. This is usually done via network connections. Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms:

a. Host computer worms, and b. Network worms.

a. Host computer worms: Host Computer worms are entirely contained in the computer. They run on and use network connections only to copy themselves to other computers. The original host computer worm terminates itself after launching a copy on another host computer. There is only one copy of the worm running somewhere on the network at a given moment. These are also called rabbits.

b. Network worms: Network worms consist of multiple parts called segments. Each Network worms running on different machines and perform different actions. These types of worms use the network for several communication purposes. Network worms have one main segment. It coordinates the work of the other segments. These are sometimes called octopuses.

Chapter–6
Hacking

1. What is hacking
2. What are Hacking Tools
3. Legal Issue of Hacking
4. International Scenario

1. What is Hacking:

Hacker is a computer programmer. Today this term is used for those computer programmers who use computers to commit crime. Hacking raises several legal issues and jeopardizes privacy and security. It raises questions about the security of the government, business, and private companies. It is argued that governments and businesses are already too dependent on computers. Institutions like research centers, defense organizations, financial networks, and educational networks are ideal targets for hackers. Individuals can suffer the consequences of malicious hackers when they trespass and damage computer systems. They regulate our lives or access into personal and confidential information.

Hacking started with telephone technology. In the USA, young men hacked into the telephone system. Telephone hackers employed different methods to accomplish this task. There were hand-held electronic devices that transmitted digital sounds or tones. Hackers altered these tones. They programmed in the sounds of coins being inserted into a public telephone. Hackers went to a public telephone, dialed a number and obtained free telephone service at most pay telephones.

2. What are Hacking Tools:

The following tools and techniques used by Hackers.

a. Denial of service attacks:
b. Distributed denial of service attacks
c. Ping of death attacks
d. Email bombing
e. Trojans

f. Viruses

a. Denial of service attacks: Denial of Service (DoS) is simple denial of service to others. Here computer workstation or server is unable to provide service to others due to input data overload. The system can not work and the system crushed. This situation is called Denial of service attacks.

b. Distributed denial of service attacks: Distributed DoS attacks are interesting and a new phenomenon. Here the perpetrators are many. They are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer. The victim's servers can not support the excess demands. This makes the server crash.

c. Ping of death attacks: The Ping of Death is a large Internet Control Message Protocol (ICMP) packet sent by a computer workstation to a target. The target receives the ping in fragments and starts reassembling the packet. When the size of the packet has become too big for the buffer then it overflows. This causes unpredictable results to make the system hangs. This is called Ping of death attacks.

d. Email bombing: Email bombing is a phenomenon that crashes the servers or overloads the networks by sending huge amounts of junk email. Due to this huge junk emails the network system and server stop functioning. This phenomenon is termed as email bombing.

e. Trojans, (for details See Chapter – 14.)

f. Viruses, (for details See Chapter – 12.)

3. Legal Issue of Hacking:

The act of hacking is nothing but the combination of criminal trespass and mischief. So hacking should have legal implications. It becomes a subject matter of cyber law.

Trespass: The Penal Code, (Bangladesh) Section 441 defines Trespass. It states that: "whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit criminal trespass.

Mischief: The Penal Code, (Bangladesh) Section 425 defines Mischief. It states that: "whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility or affects it injuriously, commits mischief".

Applying the above sections to hacking would be correct if the following issue could be resolved unambiguously: whether information residing in a computer resource is "property" as envisaged by the Penal Code of Bangladesh and India.

4. International Scenario

Here is a brief description of laws relating to hacking worldwide:

1. The United Kingdom: According to the Computer Misuse Act of 1990, a person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held within a computer or if the access he intends to secure is unauthorized. The 1990 act failed to include eavesdropping and voyeurism, although criminal liability starts at an early stage. The Computer Misuse Act covered employees accessing more information than they should be, using terminals at work. Most nations do not have this statute even though employee hacking is one of the most common acts. One important restriction in the UK is that data must be protected by security measures for a hacker to be prosecuted for trespass.

2. Germany: German law dictates three years or less in prison for any person who obtains information (data) not meant for him/her which was protected by security measures. The German parliament defined data as stored or transmitted electronic/magnetic information. This definition of data allows messages sent by e-mail or the Internet to be protected as private.

3. Norway: Citizens of Norway are subject to punishment similar to Germany's when a person is caught breaking a protection or obtaining unauthorized data and programs stored or transmitted by electrical or other technical means.

4. Netherlands: The unique thing about Dutch law is that it can be broadly applied to indict a larger number of hackers. Dutch law makes it illegal to "breach computer peace", which is one of the world's

loosest defined hacking laws. Hacking will get Dutch citizens up to four years in prison and fines not to exceed 25,000 guilders.

5. Poland: Polish law takes a strong stand against eavesdropping. The 1993 Computer Criminal Code covers eavesdropping; viewing unauthorized data, disclosure of confidential data to a third party, and also takes measures to protect privacy. The only drawback is that the victim must initiate prosecution on an application, which slows down prosecution.

Chapter–7
Cyber Terrorism

1. **What is Cyber Terrorism**
2. **Definition of cyber terrorism**
3. **What is Electronic Threat**
4. **Why computers are so vulnerable**
5. **Complexity of computer system**
6. **Who is cyber criminal**
7. **Global Cyber Terrorism**
8. **Legal Issues**
9. **Definition of the terms Used**
10. **Major Cyber Terrorism Incidents**
11. **Encryption used by terror**
12. **Famous cases on encryption technologies**

1. What is Cyber Terrorism:

Cyber terrorism is the disruptive activities, or the threat in cyber space. The intention of the cyber terrorism is to create crime in social, ideological, religious, political or similar objectives. The use of computers and the Internet by terrorists within the ambit of cyber terrorism may be termed as cyber terrorism. A cyber crime is a domestic issue but it may have international ramifications. Accordingly the cyber terrorism is an international issue but it may have domestic ramifications.

A. Illustrations:

1. Suppose due to widespread rioting of a country, the premises of some Internet Service Providers were damaged. Internet access to millions of people was cut off. This is not an act of cyber terrorism. Here cyber space activities have been disrupted. But this disruption is a consequence of a conventional terrorist activity. So, the use of computers and the Internet by terrorists within the ambit of cyber terrorism is highly undesirable and this must be considered as cyber terrorism. Accordingly the use of telephones by terrorists would give rise to "telephone terrorism".

2. If a killer is hacked into the hospital computer network and altered the prescribed medicines, then it would be an act of cyber terrorism.

3. In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise." This is not an act of cyber terrorism. The normal activities of the ISP in cyber space have been disrupted by using a preplanned methodology. The intention of the attacker was not political, social, religious, ideological or other similar objectives. The intention was to punish the ISP for interfering with the activities of the attacker. This is not an act of cyber terrorism.

4. In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestor's also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders. They threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the web-site for the Euskal Herria Journal, a New York-based publication. This publication had been supporting Basque independence. Protestors said IGC supported terrorism. Because a section on the Web pages contained materials on the terrorist group ETA. The terrorist group ETA. claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

This was an act of cyber terrorism. The normal activities of the ISP in cyber space had been disrupted by using preplanned methodology and the intention of the attackers was a political objective.

B. Legal Aspect of Cyber Terrorism:

To tackle this global phenomenon of the abuse and misuse of computers and the Internet, an international convention, is needed. The UK Terrorism Act 2000 is a step in the right direction. The Act includes cyber terrorism as a conventional terrorism. However it is essential that cyber terrorism is to be considered as a separate issue and not as a part of conventional terrorism.

2. Definition of Cyber terrorism:

People of today's technological civilization has already supported by Computer crime. This is an unbelievable experience. Computer

viruses, worms, Trojans, denial of service attacks, spoofing attacks and E-frauds are the most dangerous threat of cyber terrorism.

Cyber crime is an unlawful act wherein the computer and Internet. The computer and Internet is either a tool or a target or both. But cyber terrorism has more detailed definition.

Adv. Rohas Nagpal defined the cyber terrorism as follows:

"Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."

3. What is Electronic Threat:

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced a special type of loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. At this Jacquard's employees became fear 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.

The abacus was the earliest form of a computer that has been used since 3500 B.C. in India, Japan and China. The era of modern computers has begun with the analytical engine of Charles Babbage. Now a computer is capable of performing a billion operations per second.

Cyber crime is an evil activity. The growing dependence on computers in modern life gave birth of cyber crime. In a day and age everything from microwave ovens and refrigerators to nuclear power plants is being run on computers. So cyber crime has assumed sinister implications on the computer world and the human society.

So electronic threat can be defined as, **"Today Computer and ICT (Information and Communication Technology) are used by the terrorist. They are doing terrorist activity with the help of this technology. Computers and Information Technology is very much vulnerable. The whole world depends on this technology. The dependence increases day by day. For this increased dependence the terrorist threat also increasing day by day. For example critical infrastructures are one of the main targets of the electronic threat. So the terrorist activity by using the computer and ICT is called Electronic threat."**

4. Why computers are so vulnerable:

Computers and ICT (Information and communication Technology) are highly advanced technology devices. These are extremely vulnerable. Because computers can store huge amounts of data in small spaces. Millions of pages of written matter can be stored in single CD ROM. Stealing tones of printed information are really difficult. But to carry a CD ROM containing tones of information is much easier. The bank's servers are virtually control hundreds of billions of Dollars. To break servers are easier. The strongest firewalls and biometric authentication systems may be cracked at any time. A secret logic bomb and key loggers can steal access codes, advanced voice recorders and retina imagers. Computers are very sophisticate, sensitive and highly technical useful device for the mankind nowadays. So computer is so vulnerable.

5. Complexity of computer system:

Computer operating systems are composed of millions of lines of code. Individual cannot claim to understand the security implications of every bit of these computer instructions. Hackers can easily exploit the numerous weaknesses in operating systems and security products of computer. The hackers find out weakness to exploit and the operating system manufacturer patches it up and the cycle goes on and on. It is far easier to find weaknesses in existing operating systems rather than designing and developing a secure operating system. So computer system is very complex, highly technical and intimately related with human resource development and the civilization. The impact of computer system upon the human society is tremendous and full of complexity.

6. Who is cyber criminal:

The following four types of cyber criminal are detected. A brief description has given below:

a. Kids (age group 9-16)

b. Organized hacktivists

c. Disgruntled employees

d. Professional hackers (corporate espionage)

a. Kids (age group 9-16):

It is really true that most amateur hackers and cyber criminals are young children. To them it is a matter of pride to have hacked into a computer system or a website. They are doing these to appear really smart among their friends. These young rebels commit cyber crimes but they don't know that they are doing anything illegal.

b. Organized hacktivists:

Organized activists are doing cyber crime for particular political motive. The other reasons may be social activism, religious activism, etc. The 2001 cyber attacks disrupted approximately 200 prominent Indian websites. This had done by a group of hackers known as Pakistani Cyber Warriors. This is an example of political activists.

c. Disgruntled employees:

The displeased employees can commit cyber crime very easily. With the increase in dependence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire systems down.

d. Professional hackers (corporate espionage):

The corporate world is heavily dependent upon computers for storing sensitive information. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. They are doing this for gaining access to important documents.

7. Global Cyber Terrorism:

Computer crime has hit mankind with unbelievable severity. In the past, hackers have taken down national defense systems, taken control of a huge dam, shut down large segments of America's power grid, and silenced the command and control system of the US Pacific Command in Honolulu, disrupted troop deployments during the Gulf War etc. It is difficult to distinguish between cyber crime and a domestic issue. Cyber terrorism is an international issue. But it may have domestic ramifications. Cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both. Below some example of global cyber terrorism:

1. Osama bin Laden: The alleged mastermind behind the September 11 attack on the World Trade Center in the USA is believed to use steganography and 512-bit encryption to keep his communication channels secure.

2. Ramsey Yousuf: He was behind the bombing the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995.

3. Leary: He was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.

4. The Cali cartel: This cartel is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

5. The Dutch under world: Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops serve as an unmarked police / intelligence vehicles database.

6. The Italian mafia: Strong encryption is the criminal's best friend and the policeman's worst enemy. Some of the famous cases of criminals using encryption technologies are:

1. Aum Shinri Kyo (Supreme Truth) Case: On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more. Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever. It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life! The records of the cult had been stored in encrypted form (using RSA asymmetric algorithm) on computers. The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related plans of the cult to cause mass deaths in Japan and USA.

2. Bolivian terrorist's case: In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel. A raid on one of the hideouts of the terrorists' yielded information encrypted using symmetric encryption. A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

3. James Dalton Bell case: James Bell had launched a vendetta against the Internal Revenue Service (IRS) of the USA. His activities included intimidating IRS officials, rewarding those who killed selected government employees and contaminating an area outside IRS premises in many states of the USA. After his arrest, the investigators were able to decrypt PGP encrypted messages that he had received only because he divulged the pass phrase to his private key.

4. Kevin Paulson case : Kevin Paulson was a skilled hacker who rigged radio contests and burglarized telephone-switching offices and hacked into the telephone network in order to determine whose phone was being tapped and to install his own phone tapping devices. Paulson had encrypted files documenting everything from the phone tapping he had discovered to the dossiers he had compiled about his enemies. The files had been encrypted several times using the Data Encryption Standard. A US Department of Energy supercomputer took several months to find the key. The result yielded nearly ten thousand pages of evidence.

8. Legal Issues

The legal issues can be classified as follows:

1. Unauthorized Access
2. Computer Espionage
3. Computer Sabotage
4. Denial of Service Attack
5. Offensive Information
6. Cryptography

1. Unauthorized Access : The new law concept of unauthorised access is sometimes compared to the traditional law concept of trespass. However, in most countries, this traditional law concept cannot be stretched to protect information stored in computers. To fill in this lacuna, several countries have enacted legislations pertaining to unauthorized access of computers. These include

Australia: Part VI A of Crimes Act, 1914
Bangladesh : Bangladesh Information Technology Act (Proposed)
Canada: Article 342.1 Criminal Code
Denmark: Section 263 (2) and (3) Penal Code
Finland: Chapter 38 Section 8 of the Penal Code, amended in 1990
France: Article 462-2 Criminal Code, amended in 1988
Germany: Section 202a Penal Code
Greece: Article 370 C (2) Criminal Code, amended in 1988
India: Section 43 (a) of the Information Technology Act, 2000
Luxembourg : Article 509-1 Penal Code, amended in 1993
The Netherlands: Article 138a (1), (2) Criminal Code, amended 1992
Norway: Section 145 Penal Code, amended 1987

Spain: Article 256 Criminal Code 1995

Sweden: Section 21 Data Protection Act

Switzerland: Article 143bis Criminal Code

The United Kingdom: Sections 1, 2 Computer Misuse Act 1990

The United State of America

The Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510. 2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984, 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as various state laws.

Japan

In Japan, unauthorized access is, also after the criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g. as obstruction of business (Article 234-2 Penal Code) or theft of electricity (Article 245, 235 Penal Code).

Austria

In Austria, unauthorized access is punishable under special circumstances under the aspects of data protection (Section 49 Data Protection Act) and alteration of data (Section 126a Criminal Code) or at least attempt thereof do not have special criminal law provisions against unauthorized access. The laws relating to unauthorized access reflect divergent approaches ranging from provisions that criminalize "mere" access to computer systems Australia, Denmark, England, Greece and the majority of states of the USA. To those punishing access only in cases where the accessed data is protected by security measures: Germany, the Netherlands, Norway stored in a protected system India, Singapore, and USA

Spain

Some countries E.g., Finland, the Netherlands, India, and the United Kingdom combine several of these approaches with a basic unauthorized access offence and the creation of qualified forms of access carrying more severe sanctions. Some laws like those of Singapore, Section 8 of the Computer Misuse Act

Canada : Section 342.1 of the Criminal Code

USA

As per USA Title 18 Section 1030 (a) (6) of the United States Code "whoever ... knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorization". Californian Law penalizes one who

"knowingly and without permission provides or assists in providing a means of accessing a computer"; see Californian Penal Code Section 502 (c) (6). Criminalize preparatory acts such as "password swapping".

2. Computer Espionage : The fact that legal provisions developed for tangible property cannot be easily applied to intangible property is made apparent by an analysis of the applicability of traditional trade secret protection law to electronic records. Theft of corporeal information (e.g. books, papers etc, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic record are copied quickly, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner". The laws of countries like

Austria: Section 127 Criminal Code

Bangladesh: Section 378 of Penal Code

Belgium: Section 461 Penal Code

Germany: Sections 242 & 246 Penal Code

Greece and Italy

Sections 624, 646 Penal Code do not apply the traditional provisions on theft and embezzlement to the unauthorized "appropriation" of electronic information, as they require that tangible property be taken away with the intention of permanently depriving the victim of it.

Japan

Article 235, 252, 253 Penal Code., the definition of the intention of unlawful appropriation has been widened, and includes the intent to use property only temporarily; nevertheless, Japanese law still requires the taking of tangible property and cannot be applied if data are accessed via telecommunication facilities e.g. the Internet.

India

Section 378, Indian Penal Code; the definition of theft mandates that "movable" property is being taken out of the possession of a person without his consent. Although this would apply to theft of electronic information stored in tangible media (e.g. hard disks, CD ROMs etc), it would not apply to data accessed via telecommunication facilities. To protect trade secrets by prohibiting certain acts of obtaining information, either by provisions of the penal code or by penal or civil provisions of acts against unfair competition.

Austria: Sections 11, 12, 19 of the Act against Unfair Competition and Sections 122-124 Criminal Code;

Germany: Sections 17, 18, 20 of the Act against Unfair Competition;

Finland: Chapter 30 Sections 4-6 of the Penal Code amended 1990;

France: Section 418 Criminal Code; for Italy. Section 623 Penal Code;

Spain: Articles 278, 279, 280 Criminal Code 1995.

Canada, Denmark: The qualifications in Section 263 and 264 Penal Code, amended in 1985.

Germany: Sec- 17 of the Act against Unfair Competition, amended in 1986

Netherlands: Article 138a (2) of the Dutch Criminal Code

Sweden: Section 21 Data Protection Act, chapter 10 Section 5 Criminal Code, Protection of Trade Secrets Act 1990

United Kingdom and the United States: The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839)

3. Computer Sabotage : Traditional legal provisions for damage to property, vandalism and mischief were developed to protect tangible objects and hence their application to electronic information poses several challenges.

Austria: Section 125 Penal Code

Bangladesh : Bangladesh Information Technology Act.

Belgium: The criminal codes, Sections 528, 559 Penal Code

Canada: The criminal codes, Sections 428, 430 Criminal Code

Denmark: Section 291 Penal Code

Germany: Section 303 Penal Code

Italy: Sections 420 & 635 Penal Code

Japan: Articles 258-261 Penal Code and in addition Articles 233, 234 concerning obstruction of business

Netherlands: Section 350 Criminal Code

Norway: Section 291 Penal Code

Spain: Articles 547 et seq. of the old Criminal Code

Sweden: Chapter 12 Section 1 Criminal Code

In cases when data is not recorded on corporeal carriers but is merely transmitted. In order to clarify the situation, legislation has been enacted.

Austria: Section 126a Penal Code

Canada: Section 430(1.1) Criminal Code

Denmark: Section 193 Penal Code, amended in 1985

Germany: Sections 303a and 303b Penal Code

Finland: Chapter 35 Sections 1-3, amended 1990, chapter 34 Section 1 Para. 2 Penal Code, amended 1995

France: Articles 462-3 and 462-4 Criminal Code

India: Section 66 of the Information Technology Act, 2000

Japan: Articles 234-2, 258 & 259 Penal Code

Netherlands: Articles 350a, 350b Criminal Code

Spain: Article 264.2 Criminal Code 1995

Sweden: Section 21 Data Protection Act

Switzerland: Article 144bis Criminal Code

United Kingdom: Section 3 Computer Misuse Act 1990

United States of America: Section 18 U.S.C. § 1030 (a) (5), as well as various state laws.

In these countries the statutes use different legislative techniques. Finland has amended the traditional statutes on mischief, vandalism or damage to tangible property.

Japanese law covers all kinds of documents and not only computer-stored data. Austria, Germany, France, India, Japan, the Netherlands, New Zealand, Spain, the United Kingdom specifically protect the integrity of computer-stored data. Some legal systems also include specific qualifications for computer sabotage leading to the obstruction of business or of national security.

Independent statutes, which protect the integrity of computer-stored data, have the advantage that they can include the destruction or erasure of computerized data and their alteration or manipulation as well as the interference with the lawful use or access of data. Such comprehensive statutes can be found in Austria, Canada, Germany, India, Singapore, Luxembourg and France.

The Indian law specifically addresses computer viruses and imposes civil Section 43 (c) of the Information Technology Act, 2000 provides for damages up to Rs 1 crore and criminal liabilities and Section 66 of the Information Technology Act, 2000 applies if the virus causes any damage.

Computer virus defined as "any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is

executed or some other event takes place in that computer resource. or computer contaminant. "Computer contaminant" has been defined as any set of computer instructions that are designed-

(a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network.

Six US states have laws specifically addressing the virus problem. The six US states are **California, Illinois, Maine, Minnesota, Nebraska, and Texas.**

Italy ; The new Italian law Section 614 of the Criminal Code, introduced in December 1993 criminalizes the introduction, communication or passing on of a data processing program which was the purpose or the effect of damaging a data processing or telecommunication system or its data or programs or of interrupting or altering its operation.

Netherlands ; The new Dutch provision covers "any person who intentionally or unlawfully makes available or distributes any data which is meant to do damage by replicating itself in an automated system, however, shall not be an offence to carry out the act ... with the object of limiting damage resulting from such data."

Switzerland laws is described, "Anyone, who creates, imports, distributes, promotes, offers, makes available, circulates in any way, or gives instructions to create programs, that he/she knows or has to presume to be used for, unauthorized deleting, modifying or rendering useless of electronically or similarity stored or transmitted data, will be punished".

4. Denial of Service Attack: The following countries contain specific clauses relating to denial of service attacks.

Australia ; Section 76C Crimes Act 1914

Canada ; Section 430(1.1) Criminal Code

Germany ; Section 303b Criminal Code

India ; Section 43(f) Information Technology Act, 2000

Singapore ; Section 7, Computer Misuse Act

In other countries, denial of service would come under clauses relating to damage to computers or to data.

5. Offensive Information : The dissemination of racist statements, hate speech, and violence related information via the Internet has raised

numerous legal questions regarding the liability of the network service provider. The provisions of are -

Canada ; Section 318, 319 Criminal Code

Germany ; Section 111 Criminal Code

Switzerland ; Article 135 and 261, Criminal Code

Ireland ; Section 2 of the Prohibition of Incitement of Hatred Act 1989

Spain ; Article 510 and 607.2, Criminal Code

Portugal ; Articles 239, 240 Criminal Code

Sweden ; Chapter 16 Section 8 Criminal Code

UK ; Section 19 Public Order Act 1986

Many countries apply their criminal laws to illegal Internet content, e.g. pornography and hate speech, stored on foreign server. In such cases potential results were achieved.

Austria : Sections 62, 67 (2) Austrian Criminal Code

Denmark ; Section 9 Danish Criminal Code

Finland ; Section 10 Finnish Penal Code

Germany ; Sections 3, 9 German Criminal Code

India ; Section 1(2) and 75 Information Technology Act, 2000

Switzerland ; Sections 3 (1), 7 (1) Swiss Criminal Code

6. Cryptography : Argentina, Singapore, Egypt impose no control on the use of cryptography. Burma (Myanmar), Belgium, China, Hungary, India, Israel, Kazakhstan, Moldova, Pakistan, Poland, Russia, South Korea, Vietnam regulates the import and export of cryptography through a licensing regime.

Australia, Estonia, Finland, Germany, Greece, Ireland, Italy, Japan, Romania, Switzerland, United Kingdom, United States of America, there are no import controls, but export is controlled.

Belarus, Canada, Czech Republic, Denmark, France, Latvia, The Netherlands and New Zealand restrict import and export of cryptography is restricted.

Italy, India, Spain empowers the Government to order compulsory decryption of information under special circumstances.

The Coordinating Committee for Multilateral Export Controls (COCOM) was an international organization for the mutual control of the export of strategic products and technical data from member countries to proscribed destinations. The main goal of the COCOM

regulations was to prevent cryptography from being exported to "dangerous" countries - usually, the countries thought to maintain friendly ties with terrorist organizations such as Libya, Iraq, Iran, and North Korea. Exporting to other countries was usually allowed, although States often required a license to be granted.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is signed by Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, UK, USA, Bulgaria and Ukraine. It controls the export of weapons and dual-use goods (i.e. goods that can be used both for a military and for a civil purpose) like cryptography. The initial provisions were largely the same as old COCOM regulations. The Wassenaar provisions are not directly applicable: each member state has to implement them within national legislation for them to have effect.

Laws Specific to Cyber Terrorism in USA, UK and India.

1. United States of America ;

Section 814 of The Patriot Act Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. "Deterrence And Prevention of Cyber terrorism". This section amends section 1030(a)(5) of title 18, United States

Code. The amended section punishes any person who causes unauthorized damage to a protected computer. This section applies only in cases where the conduct of the accused causes or in the case of an attempted offence, if completed caused loss to one or more persons during any 1-year period.

For purposes of an investigation, prosecution, or other proceeding brought by the United States only, it includes loss resulting from a related course of conduct affecting 1 or more other protected computers aggregating at least $5,000 in value, or the actual or potential modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, or physical injury to any person, or a threat to public health or safety, or damage.

Section 816 of The Patriot Act is titled "Development and Support of Cyber security Forensic Capabilities". This section empowers the Attorney General to establish adequate regional computer forensic laboratories and

provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability to:

1. Provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyber terrorism),

2. Provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer related crime (including cyber terrorism),

3. Assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime,

4. Facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multi jurisdictional task forces, and

5. Carry out such other activities as the Attorney General considers appropriate.

9. Definition of The terms Used:

1. Protected computer means a computer –

(a) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(b) which is used in interstate or foreign commerce or communication; by either: knowingly causing the transmission of a program, information, code, or command, or intentionally and unauthorized accessing a protected computer

2. Loss: Loss means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service

3. Person: Person means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

4. Damage: Damage means any impairment to the integrity or availability of data, a program, a system, or information affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

10. Major Cyber Terrorism Incidents:

1. Iraqi hackers disrupted troop deployments during the Gulf War. In 1994, a 16-year-old English boy took down some 100 U.S. defense systems.

2. In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

3. Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electro hippies, another group of hacktivists, conducted web sit-ins against the WTO when they met in Seattle in late 1999.

4. In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA. He was in a position to release flood waters that would have inundated Mesa and Tempe, endangering at least 1 million people.

5. In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the web site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings".

6. In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications". Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

7. During the Kosovo conflict in 1999, NATO computers were blasted with email bombs and hit with denial of service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

8. In 2000, the Asian School of Cyber Laws was repeatedly attacked by Distributed Denial of Service attacks by "hactivists" propagating the "right to pornography". The Asian School of Cyber Laws has spearheaded an international campaign against pornography on the Internet.

9. In 2001, in the back drop of the downturn in US-China relationships, the Chinese hackers released the Code Red virus into the wild. This virus infected millions of computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

10. In 2001, hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, dubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures.

11. In the first six months of 2002 the hacker group GFORCE-Pakistan has conducted more than 150 reported cyber attacks against Indian targets to further its ideas on the Kashmir issue.

12. In 2002, numerous prominent Indian web sites were defaced. Messages relating to the Kashmir issue were pasted on the home pages of these web sites. The Pakistani Hackers Club, led by "Doctor Neukar" is believed to be behind this attack.

11. Encryption used by terror

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

Some examples are given below

1. Ramsey Yousef, who was behind the bombing the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995

2. Leary, who was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.

3. The Cali cartel, which is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

4. The Italian mafia that uses PGP. Strong encryption is the criminal's best friend and the policeman's worst enemy. The criminals used 512-bit symmetric encryption. Suppose that every atom in the known universe (they are estimated to be 2300) becomes a computer capable of checking 2300 keys per second, then it would take 2162 millennia to search 1% of the key space of a 512-bit key.

12. Famous cases on encryption technologies

1. Aum Shinri Kyo (Supreme Truth) Case
2. Bolivian terrorist's case
3. James Dalton Bell case
4. Dutch organized crime
5. The Vilseck case
6. Dallas drug ring case
7. Kevin Paulson case
8. Sacramento child pornography case

1. Aum Shinri Kyo (Supreme Truth) Case:

On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more. Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever. It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life.

The records of the cult had been stored in encrypted form (using RSA) on computers. The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related plans of the cult to cause mass deaths in Japan and USA.

2. Bolivian terrorist's case

In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel. A raid on one of the hideouts of the terrorist's yielded information encrypted using symmetric encryption. A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

3. James Dalton Bell case:

James Bell was arrested and charged with obstructing and impeding the due administration of the internal revenue laws of the USA. He allegedly did this by:

a. collecting the names and home addresses of agents and employees of the Internal Revenue Service (IRS) of the USA in order to intimidate them

b. soliciting people to join in a scheme known as "Assassination Politics". Under this scheme those who killed selected government employees, including tax collectors, would be rewarded;

c. using false Social Security Numbers to hide his assets and avoid taxes;

d. contaminating an area outside IRS premises in many states of the USA with Mercaptan (a stink gas).

Investigators found on his computer documents relating to a plan to destroy electronic equipment with nickel-plated carbon fiber. They also found an invoice for the purchase of the fiber at his residence, and a bundle of the material at the residence of his associate, Robert East. Bell had exchanged PGP-encrypted e-mail messages with some of his associates. As part of his plea bargain, he turned over the pass phrase to his private key. This allowed investigators to decrypt messages that he had received.

4. Dutch organized crime:

Dutch organized crime syndicates use PGP and PGP fone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops serve as an unmarked police / intelligence vehicles database. In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were able to recover only in 1997.

5. The Vilseck case:

An encryption case occurring in Vilseck, West Germany involved theft, fraud, and embezzlement of U.S. defense contractor and U.S. government funds over the three-year period 1986-1988. The accused

had stored financial records relating to the crimes on a personal computer, the hard disk of which had been password protected. The police used hacking software to defeat the password protection, only to find that some of the files listed in the directory had been encrypted. They then found the encryption program on the hard disk and used brute force tools to decrypt the files.

6. Dallas drug ring case:

The Dallas Police Department in the USA encountered encryption in the investigation of a drug ring, which was operating in several states of the USA and dealing in Ecstasy. A member of the ring, residing within their jurisdiction, had encrypted his address book. He turned over the password, enabling the police to decrypt the file. Meanwhile, however, the accused was out on bond and alerted his associates, so the decrypted information was not as useful as it might have been. The police noted that the Ecstasy dealers were more knowledgeable about computers as compared to other types of drug dealers, most likely because they were younger and better educated.

7. Kevin Paulson case:

Kevin Paulson was a skilled hacker who rigged radio contests and burglarized telephone-switching offices and hacked into the telephone network in order to determine whose phone was being tapped and to install his own phone tapping devices. Paulson had encrypted files documenting everything from the phone tapping he had discovered to the dossiers he had compiled about his enemies. The files had been encrypted several times using the Data Encryption Standard. A US Department of Energy supercomputer took several months to find the key, at a cost of crors of rupees. The result yielded nearly ten thousand pages of evidence.

8. Sacramento child pornography case:

The mother of a 15-year old boy filed a complaint against an adult who had sold her son Rs 50,000 worth of hardware and software for Rs 5. The man had also given the boy lewd pictures on floppy disks. The man subsequently mailed the boy pornographic material on floppy disks and sent pornographic files over the Internet. After three months of investigation, a search warrant was issued against a man in Campbell, California, USA and the adoption process of a 9-year old boy was stopped. When the accused was arrested it was found out that he had encrypted a directory on the system using PGP. The police were never able to decrypt the files.

Chapter–8

Cyber Threat to Critical Infrastructure

1. What is Critical Infrastructure:

Critical infrastructures are those physical and cyber-based systems essential for the economy and the government. Critical Infrastructure include telecommunications, energy, banking, financial, transportation, water systems and emergency services, both government and private.

Conventionally critical infrastructures are physically and logically separate entities. But they have little interdependence. The advancement of information technology and their need to improved efficiency, these infrastructures has become increasingly automated and interlinked.

This advancement has created new dimension of vulnerabilities to equipment failures, human error, weather and other natural causes. Physical and cyber attacks are the new threat to these critical infrastructures. These vulnerabilities necessarily require flexible and evolutionary approaches towards public and private sectors to protect both domestic and international security.

So it may be defined that, **"Critical infrastructures are those physical and cyber-based systems nationally and internationally important Government or Private, Strategic or Public interest organizations using Information and Communication Technology (ICT)."**

2. Cyber Threat to Critical Infrastructure:

Information and Communication Technology (ICT), Gas, oil, telecommunication and other critical industries are the most important sectors. Almost all critical infrastructural industries are setting up IT automation and security measures to deal with their vulnerabilities, consequences, and cyber threats.

The extreme competitive business environment does not allow time for businesses to the highly volatile market. Operating and manufacturing decisions as well as designs have to approved and executed within very short period.

Critical organizations may face an unexpected demand for fuel from a particular area and comes to a decision to transfer the fuel from storage. This process can be balanced with the overall system, which needs numerous physical operating control alterations throughout the system. Companies with remotely operated systems can adjust the necessary controls and rebalance the system in seconds. Whereas companies that depend on manually operated controls cannot rapidly react to these changing needs. Today any typical refinery is almost completely automated. These automated controls assist in operating the critical organizations for the fulfillment of the necessity.

Today's vital global communications networks mostly depend on the Internet. Intranets are linked to laptops, desktops, servers, firewalls, and routers. They rely on open telecommunications, architecture of satellites, fiber optic cables, microwave, phones, pagers, m-commerce and cellular equipment. Consequently, a damage or interruption to any of this equipment can endanger the trustworthiness of the infrastructures.

Electronic threats are real and growing. This threat can cause system failures and system degradation. Threats can significantly affect the business or the infrastructure. It can cause business failure, or failure to deliver services. An inappropriate business decisions may occur if data has been changed or is not available through IT system.

The advancement of information technology made hacker tools easily available. These new tools are more sophisticated and user-friendly. This induces the computers personals making them exploitable.

Cyber crimes have hit the civilization of mankind with unbelievable speed. Hacker attacks computer and internet by using viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds hacking tools. These cyber crimes have created a tremendous storm in virtual world.

Cyber criminals have been penetrating sensitive computer and internet systems. This is extremely disturbing and unwanted. For example in 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA. He might have released floodwaters that would have endangering at least 1 million people.

Today, almost all critical infrastructures are largely dependent upon information technology. Consequently the threat of cyber attacks may have increased proportionately. Most critical industries, like oil and natural gas industry are effectively geared up to protect its facilities and resources from cyber threats.

3. Use of IT in the oil and gas sector:

The oil and gas industries are using electronic communications. They are using advanced e-control systems and e-transactions for better performance and operation. The use of high technology and faster means of communications made the business arrangements consolidated among the oil companies. Systems that control operating processes within refineries, along pipelines and in producing fields are all moving towards an open architecture. The software systems are being made available generally to handle products involving a high degree of generalization with a superficial degree of customization. The oil and natural gas industries have a common dependence on IT and telecommunication systems. It also relies on Supervisory Control and Data Acquisition (SCADA) operating systems.

The security of the operating system often is as strong as the security of the corporate network. Sensitive information is increasingly available electronically. SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed. The computer then processes this data and presents it in a timely manner. SCADA also records and logs all events into a file stored on a hard disk or sends them to a printer. SCADA warns when conditions become hazardous by sounding alarms. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control.

In the oil and gas sector, there is a great need for SCADA systems. This is because oil and gas distribution may take place through hundreds of kilometers of pipelines. It would not be practical to have dedicated manned stations to monitor and control flow. Such situations SCADA systems can be used to remotely monitor and control these processes.

The use of a SCADA system is illustrated in a project for oil transportation implemented by the Consortium of Petroleum Companies. A body was formed by the Russian Federation, Kazakhastan, Oman and a consortium of petroleum companies, to develop a single shared pipeline transport system to export oil from the Tengiz oil field in Russia to a deep-water terminal on the Black Sea.

The design includes the construction of a new pipeline from Komsomolskaya to a new marine terminal at Novorossiysk and simultaneous construction of an offshore terminal.

The pipeline runs through 1500 km of mostly unpopulated land in inhospitable conditions. The pipeline is miles away from technical support so every piece of equipment in the pump stations has to be remotely managed. A supervisor in the main station should be able to control the flow of oil in each of the remote block valves. He monitors information such as pressure loss, line breach, theft, earthquakes, cracked pipelines etc. Use of a SCADA system is indispensable to monitor and control the pipeline having 18 manned pump stations, and 87 unmanned block valves along the route.

Accordingly, a SCADA system has been installed in every pump station and block valve. The system includes a central master station and a number of remote data gathering stations. The remote stations collect data from the field and send it to the central station for processing. With the compiled information, the central station can 'see' the entire pipeline and produce instant reports or alerts for unusual conditions. A SCADA system uses complex computer networking to achieve this level of efficiency, functionality and faster communication. These networks are, however, vulnerable to sabotage and disruption by hackers. It is therefore necessary to examine the vulnerabilities and threats to such systems.

4. Cyber Vulnerabilities of oil and Gas Sector:

More reliance upon the information technology and telecommunications the oil and natural gas industries have proven themselves to be secure in the physical sense. Even in the face of natural disasters, these industries are able to minimize their damage through management control procedures. These companies' increased asset utilization, and globalization of markets, an entirely new range of weaknesses, consequences, and dangers have been introduced at present days.

Recently, all the threats facing by the oil and natural gas infrastructure could be annulled through the utilization of physical security measures. These physical security barriers can be surpassed by using electronic access methods. Numerous threats could potentially affect or erase vital information resources.

Cyber threats include hardware and software failures, human errors, disgruntled employees, external hackers, something like a merger and the

ensuing struggle to consolidate systems. The outcome of these new threats is the problem of recovery of the electronic register and supporting data. Even perfect measures of physical security cannot ensure companies' security against electronic attacks. Cyber threats and weaknesses have been present for several years. Reliance on information technology and telecommunications has increased awareness and ease of exploitation of electronic vulnerabilities made a great defence against cyber Threat.

Internet has provided a global forum for hackers, disgruntled workers, cyber terrorists, cyber activists, cyber militia, terrorist nation states, and others to exploit cyber vulnerabilities. Present technological and commercial opportunities have established a better protection for critical infrastructure and resources. Oil and natural gas industrial infrastructures have become reliant on these technologies. Adequate processes and procedures have not yet been developed to safeguard these systems. The following vulnerabilities can be identified in the use of information technology systems:

a. Shared or Joint Use Systems : Numerous corporations have created shared or joint use systems for e-commerce. Failure of even one of these systems not only has a negative impact on a member of the shared service, but also can percolate throughout the entire infrastructure, creating a sizeable vulnerability.

b. Foreign Access : Mergers within the industry are creating ownership of multi-national corporations. These activities are providing the chances for foreign or nationally owned companies to access and adversely impact the established infrastructures, creating additional electronic vulnerabilities.

5. Electronic Threats:

The following are the Electronic Threat to critical infrastructure The details are given respective chapters.

1. Hacking
2. Packet Sniffing
3. TEMPEST
4. Password cracking
5. Buffer overflow
6. Trojan
7. Viruses
8. Worms

9. Email spoofing
10. Denial of Service attacks
11. Hacktivism
12. Cyber Terrorism

6. Recent Cyber Attacks on Oil Companies:

Some cyber attacks that have been successfully carried out against oil companies in the past include: Attacks on oil companies over the last few years have totaled more than 180,000. A large number of these attacks seem to have originated from countries where terrorists groups are known to be concentrated.

In 2002, the Energy and power companies experienced significant attacks to their IT infrastructure which resulted in breakdown of systems and loss of critical data. Such breakdowns resulted in huge losses for those organizations

Using inside information technology, a disgruntled employee unauthorized accessed protective equipment electronically and changed settings. The system did not respond adequately, thereby killing 6 persons and injuring dozens more.

Using a war-dialer (a program to control a modem for automated attacks), a disgruntled ex-employee scanned hundreds of phone numbers above and below an oil company's publicly available phone numbers, looking for answering modems. On finding a connection she entered multiple returns, question marks, "HELP," and "HELLO" to probe the connection and look for clues as to the kind of connection. On acquiring a login dialog she used social engineering to determine login information and then launched a brute-force password attack. Once "inside" the SCADA system, she altered data, blocked and rerouted communications, and changed numerous settings. It cost the victim organization millions of dollars to get the systems back in line.

A disgruntled ex-employee used a port scan and ping-sweep program to identify active system ports and network IP addresses belonging to an oil company. On finding an active connection and an open port, he initiated communication using various software tools downloaded from the Internet. He subsequently issued instructions to the remote system and deleted sensitive system related to process control flow. The victim's distribution channels were disrupted for several hours.

An employee with access to sensitive computer information services was duped into running a computer "game" by an outsider with legitimate connections to the employee's company. The installed computer application

contained a Trojan horse program that opened a backdoor into the computer network. The hacker was automatically notified of the backdoor and gained access to the system. He then retrieved and exploited sensitive information enabling him to access the SCADA systems and protective equipment.

An unscrupulous competitor used public information and social engineering to obtain network traffic patterns for TCP/IP packets moving between supervisory stations and remote protective equipment and metering equipment.

A network analyzer or "sniffer" was attached to the network line to show the content of all data packets between the supervisory and remote equipment. The unencrypted data packets containing control and settings information were used in subsequent attacks on the SCADA system and the protective equipment. Due to the "ILoveYou" virus a petroleum refinery in Texas, USA was completely shut down.

7. Specific Action for better protection:

The oil and natural gas industry should take the following specific actions to protect its critical infrastructures from cyber threats. Risk assessment before deciding on cyber security measures, every organization must conduct vulnerability assessments of its own systems and operations as well as those of its associates, partners, vendors etc. Subsequent to the implementation of a cyber security policy, such assessments should be carried out on a regular basis to identify any new vulnerability.

a. Information Assurance Process: Industry and government should solicit the creation, adoption, and execution of global IT management procedures to lower vulnerabilities of the critical electronic systems. A good example of such a process is the International Standards Organization (ISO) 17799, "The Standard for Information Security Management".

b. Response and Recovery Planning: Companies that only focused on natural disaster planning n ''must have plans in place to deal with a cyber attacks. Rather than simply restoring services, oil companies must plan to save lives, and save the company in the event of major disruptions of services, destruction of facilities, or loss of key personnel or infrastructure. Organizations must improve the response and recovery processes established for handling electronic system disruptions. Organizations must cooperate and participate in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures resulting from natural disaster, system failure, human error, or sabotage. Additionally, the industry must account for the challenges of the new business environment, including infrastructure interdependencies, and improve response procedures to ensure

they are adequate and well coordinated with other infrastructures, and with regional, state and local emergency response programs.

c. Information-Sharing Mechanism: The oil and natural gas industry must set up a secure information-sharing system to collect, analyze, and share information regarding physical and electronic threats, newly discovered vulnerabilities, occurrences of electronic breaches of security, and solutions practices. This mechanism could also collect information from the Government, technology providers, and other information sharing establishments. In the United States, the specific type of mechanism recommended is commonly known as an information sharing and analysis center (ISAC). The Indian Oil and Natural Gas industry should develop a similar information sharing mechanism.

d. Legislative Actions: The Governments must declare the computer systems and networks involved in the oil and natural gas infrastructure as "protected systems" under relevant legislations and provide for severe punishments if any person is found accessing the systems without specific authorization. This would create the necessary deterrent to potential hackers as the penalty for unauthorised accessing or even attempting to access such systems is imprisonment up to 10 years in certain jurisdictions. Access to Law Enforcement and Intelligence Information The industry would gain immense advantage from real-time availability of vulnerability and threat information collected by the law enforcement authorities during the course of their investigation and intelligence gathering exercises.

The Government and oil consortia must encourage information sharing on a global level so that homogenous best practice policies can be evolved. A peculiar feature of cyber threats and vulnerabilities is that they are uniform across the world and depend on the electronic systems in use and not on geographical location. This makes the possibility of uniform cyber security measures a practical possibility.

e. Research and Development Activities: Government and Industry funded research should focus on the threats posed to national security by cyber attacks on vital infrastructure. The Government and Industry should work together to prioritize research on protection of critical infrastructure.

f. Training and Implementation: Companies must seek to implement sound security policies that are customized to the needs of the organizations. These policies would help create awareness amongst the personnel about potential threats to the infrastructure. The personnel need to be trained on the aspects of the security policies so as to take preventive measures to mitigate threats.

Chapter–9
Computer Port Scanning Protocol

1. What is computer port scanning
2. What is Protocol
3. Definition of Protocol
4. Unauthorized use of Computer Port
5. Legal aspects of computer port scanning
6. Elements of Port Scanning

1. What is computer port scanning:

The word 'scan' means examine carefully. It comes from the Latin word 'scandere' which means to climb or to scale. The other meaning attributed to this word is to look at all parts successfully and intently. This also includes quick examination of all parts to detect radio activity cause to be traversed by controlled beam. Port is an electronic connection that allows data to travel between a client PC and a server on the network. Scan Data can be sent by the cracker over the Internet to locate a PC or network.

Computer Port Scanning uses various open ended technologies, tools and commands to communicate with another remote computer system or network. Computer port obtains certain sensitive information about the system functions and the properties of the hardware and the software being used by the remote systems.

Ports are an entry and exit points of any computer being used to communicate with external machines. Each computer is enabled with 3 or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner and other peripherals. The important characteristics of external ports are visible to the naked eye. These ports are located at the back of the CPU Tower. Ports are used to connect various external devices.

2. What is Protocol:

Humans communicate their views to each other using same language. They generally understand each other without rigid rules of grammar or formal language frameworks. But in the case of computer

everything explicitly should be defined and structured. If computers wish to communicate with one another, they have to know in advance exactly how information is to be exchanged and precisely what the format will be. Therefore, standard methods of transmitting and processing various kinds of information are used and these methods are called protocols. Protocols are established by international agreement and ensure that computers everywhere can talk to one another. There are a variety of protocols for different kinds of information and functions. Some of common protocols are TCP, IP, UDP, POP, SMTP, HTTP, and FTP. Details given below:

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP),
3. Mail Transfer Protocol (SMTP),
4. Post Office Protocol (POP).
5. Interactive Mail Access Protocol (IMAP).
6. Hypertext Transfer Protocol (HTTP).
7. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS),
8. File Transfer Protocol (FTP),

3. Definition of Protocol:

Wikipedia a free Encyclopedia defines as:

"In order for computers to communicate with one another, standard methods of information transfer and processing have been devised. These are referred to as protocols."

4. Unauthorized use of Computer Port:

Under normal circumstances computer ports are open. Their status is said to be listening for connections. So they are ready to establish communication with other machines on a network. In such a case any external machine wishing to send data shall, unless restricted, be allowed to communicate directly with any machine.

This is definitely a very dangerous position that any computer can be accessed and controlled by many remote hosts. It is an imminent risk that computer might at anytime shut out of its control. It may start acting against the authorized user wishes and can send important files to others. So to secure access to all the ports that is open so that no

person may remotely use a port to send data to an unauthorized port in a clandestine fashion.

All port-scanning tools give the user the chance to assess the remote system for weaknesses or vulnerabilities without letting the computer administrator know about such an audit. Generally when any information is exchanged between two computer systems, some logs and records are created on both ends, as well as the users of the computers are required to participate in the exchange of information, however, in this case, the computer of one communicates with the network of another in a stealth mode that requires no dual participation or log recording.

5. Legal aspects of computer port scanning:

The (Indian) Information Technology Act, 2000, defined as:

"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking."

Under the US Computer Fraud and Abuse Act, as well as under cyber laws of other countries, the element of unauthorized access is generally found to sufficiently cover the act of port scanning. Specifically 18 USC Sec. 1030(a)(5)(B) of the American Act has been applied to the act of port scanning in a some case.

In November 2001 a federal US court has dealt with a case of port scanning in the Moulton v. VC3 case under 18 USC Sec. 1030(a)(5)(B), of the Computer Fraud and Abuse Act of America. The facts of the case were as follows. Scott Moulton was a network security consultant, who had a service and maintenance contract with the county 911 Center to perform computer network related work. He was arrested and charged with violating the Computer Fraud and Abuse Act after his port scanned the 911 center's computer network. The defendant stated that he was concerned with the security of the network and had been authorized by the county in the service contract to maintain the networks. The defendant scanned the vulnerability of the LAN network between the sheriff's office and the 911 Center and performed a series of remote port scans on the system. The system's network administrator was using

a network analyzer and a firewall system and he was able to immediately notice the port scanning activity. The Sysop then e-mailed the defendant questioning him the reason and the motive for scanning the ports.

On being challenged, the defendant behaved in a suspicious manner, by quitting the scanning activity and immediately emailed back, informing the administrator that he had a service contract with the county and he was authorized to check the security of the network. Concerned about the network's security and the act of the defendant, the network administrator then contacted the sheriff, who in turn arrested the defendant on state and federal computer crime charges.

The Information Technology Act, 2000 does not cover acts like port scanning under the offence of hacking. In certain cases the security of certain systems is utmost priority like in case of defense and strategic installations. Computer Port Scanning is covered by Section 70 of the Indian IT Act 2000. This Act provides provisions about unauthorized access of a protected system. The Bangladesh Information Technology Act (Proposed) also provides provisions about unauthorised access of protected system in section 70.

6. Elements of Port Scanning

The followings are the elements of Computer Port Scanning:
Intention.

1. Knowledge
2. Deletion, Alteration, Destruction of data
3. Wrongful Loss to Public

Computer Port Scanning will satisfy the requirements of first three elements. But the forth essential is not always met. Computer port scanning does not necessarily cause any wrongful loss in every case. Because if a network administrator scans his own network for security reasons, then he will not intend to create any wrongful loss.

Chapter–10

Cyber Crime and International Laws

1. What is the character of Cyberlaws
2. Protection of Privacy
3. Legal Protection of Intellectual Property
4. Legal Protection of Topographies
5. Databases Special Protection copyright
6. Illegal and Harmful Contents
7. Criminal Procedural Laws
8. Security Laws
9. Computer Related Economic Crimes
10. Unauthorized access
11. Computer Espionage
12. Computer Sabotage
13. Computer Forgery
14. Computer Fraud
15. Laws on Criminal Liability
    a. Violence,
    b. Hate speech,
    c. Racism
        a. Pornography
        b. Child pornography
        c. Child pornography age limit
        d. Protection of minors, actors and others
        e. Visual depictions of pornography, sound recordings
        f. Protection of mental & moral development of young
        g. Protection to adults aims of pornography
        h. Laws on Public moral standards
        i. Responsibility of Service Providers

---

1. What is the character of cyber laws:

Computer data is the main object of computer crime. Extreme mobility is the characteristic of computer data. This exceeds the

mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the world in a matter of seconds. This mobility of computer data in international computer networks makes international solutions for fighting computer crime indispensable.

Different national have the aim and strategies with to prevent computer crimes. They have created 'data havens' or 'computer crime havens'. These would create national barriers to the free flow of information and world-wide services. National solutions and restrictions for the free flow of information would be doomed to failure since the amount of data transferred in international computer networks makes controls of their content neither possible nor socially desirable. So, international and supranational aspects concerning computer crime gain becomes much more importance than in other comparable fields of crime.

Cyber law is new concept of law. It may be the new branch of law which will dominate the whole civilization of mankind. The growth and development of the law related to cyber crime in the international community tremendously proceeds with its own way. Law relating to cyber crime may be divided into the following spheres.

1. A part of cyber law may be conventional law as most of the cyber crimes are similar to conventional crimes.
2. The other laws are to be enacted by the parliament of the respective country as per their requirements.

Different countries are framing the laws. It is to be remembered that Bangladesh passed an IT policy 2002 and IT Act enacted (Proposed). So it can be said that Bangladesh is not behind the legal aspect of present Cyber law of the world. The debate between the Cyberlaws and conventional laws will determine the position of human civilization.

2. Protection of Privacy Right

Protection of privacy right is basically a reaction to the challenges of privacy caused by expanded possibilities for collecting, storing and transmitting data by new Technologies. This is the aim of legislation. On the other hand Data Protection Laws aim is to protect the right of privacy with administrative, civil, and penal regulations. Some international regulation is mentioned as below.

1. Austria in 1978: The Federal Data Protection Act of 18 October 1978, amended by laws Nos. 370 of 1986, 605 of 1987 and 632 of 1994

2. Australia in 1982: The Freedom of Information Act of 9 March 1982, as amended and the Privacy Act 1988

3, Bangladesh enacts IT Policy and IT Act (Proposed)

4. Belgium in 1992: The law for the Protection of the Private Life with Respect to the Treatment of Personal Data of 8 December 1992

5. Brazil : Article 5 (0) X of the Constitution

6. Canada in 1982: The Access to Information Act and the Privacy Act of 28 June 1982

7. Denmark in 1978 : The Private Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988 and the Public Authorities' Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988.

8. France in 1978: The Act on Data Processing, Data Files and Individual Liberties (Act No. 78-17) of 6 January 1978, amended on 11 March 1988

9. Finland in 1987 : The Personal Data File Act No. 471 of 30 April 1987, Personal Registers Act of 4 February 1987 and chapter 38 of the Penal Code (as amended 1995)

10. Germany in 1977: The Data Protection Act of 20 December 1990 (succeeding the Data Protection Act of 27 January 1977)

11. Greece in 1997: Data Protection Act (law 2472/1997), passed in April 1997

12. Iceland in 1981: The Act Concerning the Systematic Recording of Personal Data (Act No. 39/1985) of 25 May 1981

13. India in 2000: Information Technology Act, 2000

14. Ireland in 1988: The Data Protection Act (Act No. 25/1988) of 6 July 1988

15. Israel in 1981: The Protection of Privacy Law (Act No. 5741/1981) of 23 February 1981, amended in 1985

16. Italy in 1997: Law No. 675 of 31 December 1996, published in the Gazette Official 8 January 1997

17. Japan in 1988: The Personal Information Protection Act No. 95 of 16 December 1988

18. Luxembourg in 1979 and 1982: The Act Organizing the Identification on Physical and Legal Persons by Number of 31 March 1979, the Act Regulating the Use of Nominal Data in Electronic Data Processing of 31 March 1979 and the Act concerning the Protection of Privacy of 11 August 1982

19. Netherlands in 1988: The Law on the Protection of Privacy in Connection with Personal Registration of 28 December 1988 and Article 10 of the Constitution;

20. New Zealand in 1993 : The Privacy Act 1993, amended by the Privacy Amendment Act 1993 and the Privacy Amendment Act 1994

21. Norway in 1978: The Law on Personal Data Registers of 9 June 1978 (Act No. 48) amended by Law No. 55 of 12 June 1987, Law No. 66 of 20 July 1991 and Law No. 78 of 11 June 1993.

22. Portugal in 1991: Law 10/91 of 29 April 1991 on the Protection of Personal Data with Respect to Informatics, amended by Law 28/94 of 29 August 1994 and Article 35 of the Constitution

23. Spain in 1992: Art. 18 para. 4 of the Constitution and Law 5/1992 for the Regulation of the Automated Processing of Personal Data (LORTAD) of 29 October 1992, and Article 197 Criminal Code (Law No. 10/1995 of 23 November 1995) and Article 18.4 of the Constitution

24. Sweden in1973: Chapter 2 Article 3 paragraph 2 Instrument of Government (i.e., Constitution) as amended 1988; the Data Protection Act of 11 May 1973 (Law No. 289), amended 1979, 1982, 1986, 1990 and 1992.

25. Switzerland in 1992: Federal Data Protection Act of 19 June 1992

26. U.S.A. in1974: The Privacy Act 1974 (5 U.S.C. § 552a) and the Electronic Communications Privacy Act 1986 (codified at 18 U.S.C. §§ 1367, 2232, 2510-2522, 2702-2711, 3117, 3121-3127).

27. U. K. in 1984: The Data Protection Act of 12 July 1984

3. Legal Protection of Intellectual Property right:

In 1980s series of law amended to improved the protection of intellectual property right in the field of computer technology. The laws of different countries are given below.

1. Austria in 1984: Bundesgesetzblatt 1984/234, Section 1(2) No. 3 Patent Law, amended 8 June1984 and The Copyright Amendment Act 1984

Copyright Amendment Act 1993 (Bundesgesetzblatt 1993/93) as amended in Bundesgesetzblatt 1996/151

2. Bangladesh: The Copyright Amendment Act No XIX of 1984

3. Brazil in 1987: Law No. 7.646 of 18 December 1987

4. Canada in 1988: The Copyright Amendment Act 1988

5. Germany 1980: The Copyright Amendment Act of 24 June 1985 (Bundesgesetzblatt I, 1985, p. 1137) and further amendments in Second

Act to Amend the Copyright Act of 9 June 1993 (Bundesgesetzblatt I, 1993, p. 910) and Law No. 153 of 14 January 1988

6. France in 1968: Sections 6 and 11 Patent Law No. 68-1 of 2 January 1968, modified by Law No. 78-742 of 13 July 1978 and Law No. 84-500 of 27 June 1984 and Law No. 85-660 of 3 July 1985

7. Finland in 1991 : The Copyright Amendment Acts No. 34/1991 of 11 January 1991, No. 418/1993 of 7 May 1993 and No. 446/1995 of 24 March 1995

8. Germany in 1936: Section 1 (2) No. 3 and (3) Patent Law of 5 June 1936, amended on

9. Hungary in 1983: Decree No. 15 of the Minister of Culture of 12 July 1983

10. India in 1984: The Copyright Amendment Act No. XIX of 1984

11. Italy in 1939: Section 12 Patent Law No. 1127 of 29 January 1939, modified by Law No. 338 of 22 June 1979

12. Israel in 1988: Copyright Ordinance 1911 as amended in 1988

13. Japan in 1985: The Copyright Amendment Act of 7 June 1985

14. Luxembourg in 1995: The Act of 24 April 1995 amending the Copyright Act of 29 March 1972

15. Mexico in 1984: The Copyright Amendment Act No. 114 of 8 October 1984

16. Norway in 1990: The Copyright Amendment Act of 15 June 1990

17. Philippines in 1972: The Presidential Decree No. 49 of 14 November 1972

18. Spain in 1987: Law No. 22/1987 on Intellectual Property of 11 November 1987, latest version passed by R.D. 1/1996 on 12 April 1996

19. Sweden in 1989: The Copyright Amendment Act of 1989 (effective 1 July 1989)

20. United Kingdom in 1977: Section 1 (2) (c) of the Patents Act 1977 and the Copyright (Computer Software) Amendment Act 1986

21. U.S.A. in 1980: The Computer Software Copyright Act 1980 amending the Copyright Act 1974 (17 U.S.C. §§ 101, 117)

4. Legal Protection of Topographies

The development of legal protection concerning topographies is giving below:

1. Austria in 1988: The Semiconductor Protection Act (Bundesgesetzblatt 1988/372)

2. Canada in 1990: The Integrated Circuit Topography Act (S.C. 1990, c. 37)

3. Denmark in 1987 : The Act on the Protection of Semiconductor Products, Law No. 778 of 9 December 1987

4. European Commission (EC): Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24/36 of 27.01.1987

5. Finland in 1991: The Act on the Protection of Semiconductor Topographies No. 32/1991 of 11 January 1991

6. France in 1987: The Act on the Protection of the Topographies of Semiconductor Products, Law No. 87-890 of 4 November 1987

7. Germany in 1987: The Act on the Protection of Topographies of Micro-Electronic Semiconductor Products of 22 October 1987 (Bundesgesetzblatt I, 1987, p. 2294, as amended 1990)

8. India in 2000: Semiconductor Integrated Circuits Layout-Design Act, 2000

9. Italy in 1987 : The Provisions Protecting Semiconductor Product Design of 1987

10. Japan in 1985: The Act Concerning the Circuit Layout of a Semiconductor Integrated Circuit of 31 May 1985

11. Netherlands in 1987: The Act of 28 October 1987 on the Protection of Original Topographies of Semiconductor Products

12. Spain in 1988: Law on the Legal Protection of the Topographies of Semiconductor Products of 3 May 1988

13. Sweden in 1986: The Act on the Protection of the Layout-Design of the Circuitry in Semiconductor Products, Law No.1425 of 18 December 1986

14. United Kingdom in 1987 : The Semiconductor Product - Protection of Topography - Regulations 1987

15. United States of America in 1984: The Semiconductor Chip Protection Act of 8 November 1984

5. Databases Special Protection copyright

1. Austria in 1993: Copyright Amendment Act 1993 (Bundesgesetzblatt 1993/93) as amended in Bundesgesetzblatt 1996/151

2. China in 1985 : The Copyright Law of 1985

3. Canada in 1987: Section 42 Copyright Act 1087

4. Finland in 1984 : The Copyright Amendment Acts No. 34/1991 of 11 January 1991, No. 418/1993 of 7 May 1993 and No. 446/1995 of 24 March 1995 the Act Amending the Act Relating to Copyright in Literary and Artistic Works (Law No. 442) of 8 June 1984

5. France in 1985: Law No. 85-660 of 3 July 1985

6. Germany in 1997: Article 7 Information and Communication Services Act of 22 July 1997 (Bundesgesetzblatt I, 1997, p. 1870) and The Copyright Amendment Act of 24 June 1985 (Bundesgesetzblatt I, 1985, p. 1137) and further amendments in Second Act to Amend the Copyright Act of 9 June 1993 (Bundesgesetzblatt I, 1993, p. 910)

7. Italy in 1981: Law No. 406 of 29 July 1981 Concerning Urgent Measures Against the Unlawful Copying, Reproduction.

8. Netherlands in 1994: Copyright Act of 7 July 1994

9. Sweden in 1982 : Law No. 284 of 19 May 1982

10. Spain in 1995: Incorporated in Articles 270 et seq. Criminal Code 1995

11. United Kingdom in 1982 and 1988: The Copyright Act 1956 (Amendment) Act 1982 of 13 June 1982, the Copyright Amendment Act 1983 and the Copyright, Designs and Patents Act 1988 Section 107

12. USA in 1982: The Piracy and Counterfeiting Amendment Act of 24 May 1982 (17 U.S.C. § 506) and the Copyright Act as amended 1980 (17 U.S.C. §§ 502-505)

6. Illegal and Harmful Contents : (Pornography, Defamation.)

1. Bangladesh : The Information Technology Act (Proposed):

2. Germany in 1997: Section 5 of the Teleservices Act (Bundesgesetzblatt I, 1997, p. 1870) as well as Section 5 of the State Treaty of the German Länder on Media Services of 12 July 1997 (cf. Bayerisches Gesetz- und Verordnungsblatt 1997, p. 225) and Articles 1, 4, 5 and 6 Information and Communication Services Act (Bundesgesetzblatt I, 1997, p. 1870)

3. India in 2000: Section 67 of the Information Technology Act, 2000 and Section 79 of the Information Technology Act, 2000

4. United Kingdom in 1994: Criminal Justice and Public Order Act of 1994 amending the Obscene Publications Act

5. USA in 1996: Sections 501 et seq. Telecommunications Act of 1996 (the provisions are also known as "Communications Decency Act")

7. Criminal Procedural Law:

1. Austria in 1993. Strafprozeßänderungsgesetz 1993, Bundesgesetzblatt 1993/526

2. Bangladesh 1898 : The code of Criminal Procedure 1898.

3. Denmark in 1985: Chapter 71, Section 780 of the Administration of Justice Act, amended by Act No. 229 of 6 June 1985

4. Germany92 in 1996: Article 4 (17s) of the Poststrukturgesetz of 14 June 1989; Sections 90 and 92 Telekommunikationsgesetz of 1 August 1996, Bundesgesetzblatt I, 1996, pp. 1117 et seq.

5. Netherlands in 1992: Articles 125f-n Criminal Procedural Code

6. U. K. in 1984: The Police and Criminal Evidence Act 1984

7. USA and Canada in 1986, 1988 and 1997: Section 16 Competition Act; Subsections 100 (6) and 101 (5) of the Section 101 (3)-(6) Environmental Protection Act; Section 18 (2) Mutual Assistance Act; Section 487 (2.1.) Criminal Code, introduced by the Criminal Law Improvement Act 1997

8. Security Law:

The 1990s have seen the emergence of laws relating to the creation of requirements for and prohibitions of security measures. This includes minimum obligations for security measures in the interest of privacy rights or in the general public interest and prohibitions of specific security measures in the interest of privacy rights or of effective prosecution of crimes.

9. Computer Related Economic Crimes:

Computer-related economic crimes violate traditional objects in the form of new media. It is also involve in intangible objects of computer programs. So the legislation on computer related economic crimes become necessary and many countries have enacted new laws. The laws are listed below:

1. Australia in 1979 (state law): Section 408e, of Queensland Criminal Code, amended in 1979, Sections 222, 276 of Northern Territory Criminal Code, amended in 1983, Section 115 of New South Wales Crimes Act 1900 in its application to the Australian Capital Territory, as amended in 1985, the Crimes (Computers) Act No. 36 of 1988 of Victoria, additional legislation passed in the Australian Capital

Territory, the Commonwealth, New South Wales, the Northern Territory, South Australia and Victoria.

2. Austria in 1987: Criminal Code Amendment Act of 1987 (Bundesgesetzblatt 1987/605)

3. Bangladesh : The Information and Technology Act (Proposed)

4. Canada in 1985: The Criminal Law Amendment Act 1985 (S.C. 1985, c. 19)

5. Denmark in 1985: The Penal Code Amendment Act of 6 June 1985 on Data Criminality

6. Federal Republic of Germany in 1986: The Second Law for the Suppression of Economic Crime (15 May 1986) (Bundesgesetzblatt I, 1986, p. 721)

7. France in 1988: Law on Infringements in the Field of Informatics of 5 January 1988

8. Finland in 1990: Laws Amending the Criminal Code No. 769/1990 of 24 August 1990 (first phase of the total reform of the Criminal Code), and No. 578/1995 of 28 April 1995 (second phase of the total reform of the Criminal Code)

9. Greece in 1988 : Law No. 1805/88 of 30 August 1988

10. India in 2000: Information Technology Act, 2000

11. Italy in 1978 : The Amendment of 1978 to Section 420 Penal

12. Japan in 1987 : The Penal Code Amendment Act of 1987

13. Luxembourg in 1993: Law of 15 July 1993 Aiming to Reinforce the Fight against Economic Crime and Computer Fraud.

14. Malaysia in 1997: Computer Crime Law of 1997

15. Netherlands in 1992: Dutch Computer Crime Act of 23 December 1992, as amended in 1994 and 1995

16. Norway in 1987: The Criminal Code Amendment Act of 12 June 1987

17. Spain in 1995: Spain, Criminal Code 1995 (Law No. 10/1995 of 23-11-1995), especially Articles 248.2, 256, 264.2, 278

18. Sweden in 1986: Sec. 21 Data Protection Act (4–4-1973), the Criminal Code Amendment Act of July 1986 (Law No. 123)

19. Switzerland in 1994: 1994 Revision of Property Crime Provisions

20. Switzerland in 1994: 1994 Revision of Property Crime Provisions

21. U. K. in 1981: The Forgery and Counterfeiting Act of 1981 and

The Computer Misuse Act 1990 of 29 June 1990, draft for a new Section 15a Theft Act 1968

22. U.S.A. in 1978: State legislation in every state but Vermont

23. United States of America in 1984(federal level) : The Credit Card Fraud Act of 1984 (Publ. L. 98-473), The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the Computer Fraud and Abuse Act of 1986 (both codified as amended at 18 U.S.C. §§ 1029? 1030)

10. Unauthorized access :

Several countries have enacted legislations to protect unauthorized access of computers.

1. Australia in 1914: Part VI A of Crimes Act, 1914

2. Austria: Section 49 Data Protection Act, Section 126a Criminal Code.

3. Bangladesh: The Information Technology Act (Proposed)

3. Canada: Section 342.1 of the Criminal Code

4. Denmark: Section 263 (2) and (3) Penal Code

5. Finland: Chapter 38 Section 8 of the Penal Code (amended 1990)

6. France: Article 462-2 Criminal Code, amended in 1988

7. Germany: Section 202a Penal Code

8. Greece: Article 370 C (2) Criminal Code, as amended in 1988

9. India : Section 43 (a) of the Information Technology Act, 2000

10. Luxembourg: Article 509-1 Penal Code, as amended in 1993

11. Japan: The criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g. as obstruction of business (Article 234-2 Penal Code) or theft of electricity (Article 245, 235 Penal Code)

12. Netherlands: Article 138a (1), (2) Criminal Code, amended 1992

13. Norway: Section 145 Penal Code, amended 1987.

14. Singapore : Section 8 of the Computer Misuse Act

15. Spain : Article 256 Criminal Code 1995

16. Sweden : Section 21 Data Protection Act

17. Switzerland : Article 143bis Criminal Code

18. United Kingdom : Sections 1, 2 Computer Misuse Act 1990

19. United States of America: The Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984 and 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as various state laws and As per USA Title 18 Section 1030 (a) (6) of the United States Code "whoever ... knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorization." Californian Law penalizes one who "knowingly and without permission provides or assists in providing a means of accessing a computer"; see Californian Penal Code Section 502 (c) (6).

11. Computer Espionage:

These are the International Laws regarding Computer Espionage

1. Austria: Section 127 Criminal Code and Sections 11, 12, 19 of the Act against Unfair Competition, Sections 122-124 Criminal Code

2. Bangladesh: Section 378 of Penal Code

3. Belgium: Section 461 Penal Code

4. Canada: Section 263 and 264 Penal Code, amended 1985

5. Denmark: Section 263 and 264 Penal Code, amended 1985

6. Finland: Chapter 30 Sections 4-6 of the Penal Code (amended 1990)

6. France: Section 418 Criminal Code

7. Germany: Sections 242, 246 Penal Code and Sections 17, 18, 20 of the Act against Unfair Competition amended 1986

8. Greece: Sections 624, 646 Penal Code

9. India: Section 378, Indian Penal Code

10. Italy: Sections 623, 624, 646 Penal Code

11. Japan: Article 235, 252, 253, Penal Code

12. Netherlands: Article 138a (2) of the Dutch Criminal Code

13. Spain: Articles 278, 279, 280 Criminal Code 1995

14. Sweden: Section 21 Data Protection Act, chapter 10, Section 5 Criminal Code, Protection of Trade Secrets Act 1990

15. United Kingdom: The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839)

16. United States of America: The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839)

12. Computer Sabotage

These are the International Laws regarding Computer Sabotage

1. Austria: Section 125, 126a Penal Code

2. Belgium: Sections 528, 559, Penal Code

3. Bangladesh: Information Technology Act (Proposed)

4. Canada: Sections 428, 430, 430(1.1) Criminal Code

5. Denmark: Section 291, 193 Penal Code, amended in 1985

6. Finland: Chapter 35 Sections 1-3, amended 1990, chapter 34 Section 1 para-2 Penal Code, amended 1995

7. France: Articles 462-3 and 462-4 Criminal Code

8. Germany: Section 303, 303a and 303b Penal Code

9. India: Section 66 of the Information Technology Act, 2000, Section 43 (c) of the Information Technology Act, 2000 provides for damages up to Rs 1 crore (US $ 200,000). Criminal liabilities, Section 66 of the Information Technology Act, 2000 applies if the virus causes any damage.

10. Italy: Sections 420, 635 Penal Code, The new Italian law (Section 614, Criminal Code, introduced in December 1993.

11. Japan: Articles 258-261 Penal Code and in addition Articles 233, 234 concerning obstruction of business, Articles 234-2, 258, 259 Penal Code

12. Netherlands: Sec350 Criminal Code, Articles 350a, 350b Criminal Code

13. Norway: Section 291 Penal Code

14. Spain: Articles 547 et seq. of the old Criminal Code

15. Sweden: Chapter 12 Section 1 Criminal Code, Section 21 Data Protection Act

16. Spain: Article 264.2 Criminal Code 1995

17. Switzerland: Article 144bis Criminal Code

18. United Kingdom: Section 3 Computer Misuse Act 1990

19. United States: Sec-18 U.S.C. § 1030 (a) (5), as well as various state laws

13. Computer Forgery :

These are the International Laws regarding Computer forgery

1. Austria : Section 223 Penal Code

2. Australia: Section 321 Criminal Code

3. Bangladesh: Chapter 18 of the Penal Code

4. Belgium: Section 193 Penal Code

5. Canada: Section 321 Criminal Code

6. Finland: Chapter 33 Sections 1-6 of the Penal Code, amended 1990

7. France: Sec- 145 Penal Code, Article 462-5 and Article 462-6 Penal Code

8. Germany: Section 267 Penal Code, Sections 269, 271, 273, 274, 348 Penal Code, amended in 1986

9. Greece : Article 13 C Criminal Code

10. Italy: Sections 476, 485 Penal Code

11. India : Chapter 18 of the Indian Penal Code

12. Japan : Articles 7-2, 157, 158, 161-2 Penal Code

13. Luxembourg : Articles 509-4 and 509-5 Penal Code

14. Norway : Sections 179, 182 Penal Code

15. Switzerland: Sections 110, No. 5; 251-7, 317, Penal Code

16. United Kingdom : Sections 179, 182 Penal Code

14. Computer Fraud

These are the International Laws regarding Computer fraud

1. Australia: Section 148a Criminal Code

2. Austria: Section 146 Penal Code and Section 148a Criminal Code

3. Bangladesh: Section 378, 415 of the Penal Code and Information Technology Act 2005

4. Belgium : Section 496 Penal Code

5. Canada : Section 380 Criminal Code

6. Denmark: Section 279 Penal Code & Section 279a Penal Code, amended in 1985

7. France: Section 405 Penal Code

8. Finland : Chapter 36, Sec- 1, para 2 of the Penal Code, amended in 1990

9. Germany: Sections 242, 246, 263, Penal Code & Section 263a Penal Code, amended in 1986

10. Greece: Article 386 A Criminal Code, amended in 1988

11. India: Section 378, 415 of the Indian Penal Code and Section 43(h) of Information Technology Act, 2000

12. Italy : Section 624, 640 of Penal Code

13. Japan: Articles 235, 246, 246-2, 252, 253 of Penal Code

14. Luxembourg: Articles 235, 252, 253, of Penal Code and Articles 509-2 and 509-3 Penal Code, amended in 1993

15. Netherlands: Section 326, 326c of Criminal Code

16. Norway: Section 270 (2) Penal Code, amended in 1987

17. Sweden: Chapter 9, Section 1, para 1 of Criminal Code and Chapter 9, Section 1, para 2 of Criminal Code, amended in 1986

18. Spain: Articles 248.2, 239 of fine Criminal Code 1995

19. USA: Section 18 U.S.C. § 1030 (a) (4) (1988) and various state laws

15. Laws on Criminal Liability:

These are the International Laws regarding laws on criminal liabilities:

a. Violence,
b. Hate speech,
c. Racism
d. Pornography
e. Child pornography
f. Child pornography age limit
g. Protection of minors, actors and others
h. Visual depictions of pornography, sound recordings
i. Protection of mental & moral development of young
j. Protection to adults aims of pornography
k. Laws on Public moral standards
l. Responsibility of Service Providers

a. Violence:

1. Bangladesh : Section 292 of Penal Code.

2. Canada : Section 318 Criminal Code

3. Germany: Section 111 Criminal Code

4. Switzerland : Article 135 Criminal Code

b. Hate speech:

1. Canada: Section 319 Criminal Code

2. Ireland: Section 2 of the Prohibition of Incitement of Hatred Act 1989

3. Spain: Article 510 Criminal Code

c. Racism

1. Spain: Article 607.2 Criminal Code

2. Portugal: Articles 239, 240 Criminal Codes

3. Sweden: Chapter 16 Section 8 Criminal Code

4. Switzerland: Article 261, Criminal Code

5. United Kingdom: Section 19 Public Order Act 1986

d. Pornography

1. Germany: Section 184 Criminal Code

2. Spain: Article 186 Criminal Code

3. Italy: Sections 528, 529, 725, 726 Criminal Codes

4. India: Section 292 of the Indian Penal Code

5. Belgium: Articles 383, 384, 383 Criminal Code

e. Child pornography:

1. Austria: Federal Act of 31 March 1950 against Obscene Publications and for the Protection of the Young People and Section 207a (3) Criminal Code

2. Bangladesh: (Bangladesh) Information Technology Act.

3. Belgium : Article 383 bis Penal Code

4. Finland: Prevention of Dissemination of Indecent Publications Act 1927

5. Germany: Section 184 (5) Criminal Code

6. India: Indecent Representation of Women (Prevention) Act and section 67 of the Information Technology Act, 2000

7. United Kingdom: Obscene Publications Act 1959

8. United States of America: 18 U.S.C. § 2252 (a) (4) punishes possession only if at least three publications with child pornographic content are possessed.

f. Child Pornography age limit

Austria and Germany : 14 years

France and Poland : 15 years

Belgium, Switzerland, Netherlands, Norway, UK : 16 years

Canada, Sweden, and the USA : 18 years

g. Protection of minors, actors and others

1. Austria : Section 207a Criminal Code

2. Bangladesh : Section 293 of Penal Code

3. Belgium : Article 383 Penal Code

4. Canada : Section 163.1 Criminal Code

5. Denmark : Section 235 Criminal Code

6. France : Article 227-23 New Penal Code

7. Germany : Section 184 (3), 184 (4) Criminal Code and Law on the Dissemination of Publications and Other Media Morally Harmful to Youth

8. India : Section 293 of the Indian Penal Code

9. Ireland: Section 2 Child Pornography Act 1996

10. Netherlands: Section 240b Criminal Code

11. Norway : Section 211, 211 (6) of Criminal Code

12. Spain: Article 189 1 Criminal Code

13. Sweden: Chapter 16 Section 10a, 10b (2) of Criminal Code

14. United Kingdom: Sec 1 of the Protection of Children Code 1978 as amended by the Criminal Justice and Public Order Act 1994United States of America 18 U.S.C. § 2252 and Protection of Children Act 1978

15. United States of America: The Communications Decency Act 1996 and Laws on telecommunication are also applicable.

h. Visual depictions of pornography, sound recordings

1. Austria: Section 207a (3) Criminal Code

2. Bangladesh: Section 294 of Penal Code and Information Technology Act 2005

3. Belgium: Article 383 Penal Code

4. Canada: Section 163 Criminal Code

5. Denmark: Section 235 (2) Criminal Code

6. Germany: Section 11 (3), 184 (1) of Criminal Code

7. India: Section 294 Indian Penal Code and Section 67 Information Technology Act, 2000

8. Ireland: Section 1 of the Child Pornography Act 1996 & 1978 amended by the Criminal Justice and Public Order Act 1994

9. Norway: Section 211 (1) (d) Criminal Code

10. U. K. : Section 7 (4) of the Protection of Children Act

i. Protection of mental & moral development of young

1. Bangladesh: Section 293 of Penal Code

2. Canada: Section 163 Criminal Code

3. Denmark: Sections 232, 233, 234 Criminal Code

4. Germany: Sec- 184 (1) Criminal Code, Sections 1, 21 of the Law on the Dissemination of Publications and Other Media Morally Harmful to Youth

5. Greece: Article 30 of the Law 5060/1931 related to the Punishment of Immodest Behavior

6. India: Section 293 of the Indian Penal Code

7. Spain: Article 186 Criminal Code

8. Sweden: Chapter 16 Section 12 Criminal Code

9. Switzerland: Article 197 Criminal Code

j. Protection to adults aims of pornography

1. Finland: Chapter 20 Section 9 Penal Code, Section 1 para. 1 of the Prevention of Dissemination of Indecent Publications Act 1927

2. France: Articles 227-24, 227-28, R 624-2 New Penal Code

3. Greece: Articles 29 (1), 30 of the Law 5060/1931 related to the Punishment of Immodest Behavior

4. Germany: Sec 184 (1) Criminal Code, Section 1 and 21 of the Law on the Dissemination of Publications and Other Media Morally Harmful to Youth

5. Ireland: Section 2 (1) (b) of the Child Pornography Act 1996

6. Japan: Article 175 Penal Code

7. Norway: Sections 376, 377 Criminal Codes

8. Sweden: Chapter 16 Section 10b and Section 12 Criminal Code

9. United Kingdom: Criminal Justice and Public Order Act 1994

k. Laws on Public moral standards

1. Austria: Sections 62, 67 (2) Austrian Criminal Code

2. Bangladesh: Section 292-294 of the Penal Code and Information Technology Act

3. Denmark: Section 9, 232 Criminal Codes

4. France: Article R 624-2 New Penal Code

5. Finland: Section 10 Finnish Penal Code

6. Germany: Sections 3, 9 German Criminal Code

7. Greece: Article 29 (1) of the Law relating to the Punishment of Immodest Behavior

8. India: Section 292-294 of the Indian Penal Code, section 1(2), 67, 75 of the Information Technology Act, 2000 and the Indecent Representation of Women (Prevention) Act

9. Italy: Constitution (Article 21 Section 6) calls for the protection of public morality

10. Netherlands: Section 240 Criminal Code

11. Norway: Sections 376, 377 Criminal Codes

12. Switzerland: Sections 3 (1); 7 (1) Swiss Criminal Code

l. Laws on responsibility of Service Providers

1. Austria: Section 43 Telecommunications Act

2. Bangladesh: Information Technology Act

3. Germany: Section 5 Teleservices Act and Section 5 State Treaty of the German Länder on Media Services

4. India: Section 79 Information Technology Act, 2000

5. Netherlands: Articles 53, 54, 418, 419 Criminal Code

6. Sweden: Electronic Mediation Services Act

7. USA: 47 U.S.C. § 223, 47 U.S.C. § 230

Chapter–11
Virus

1. What is Viruses?
2. Kind of Viruses
- **a. Stealth virus**
- **b. Polymorphic virus**
  - **a. Fast and slow infectors**
  - **b. Sparse infector**
  - **c. Companion virus**
  - **d. Armored virus**
  - **g. Virus hoax**

3. World Famous Virus Incidents Since 1998
1. **Melissa**
2. **ExploreZip**
3. **Chernobyl**
   1. **VBS_LOVELETTER**
   2. **Pakistani Brain**
   3. **Stoned-Marijuana**
   4. **Jerusalem**
   5. **Cascade**
   6. **Michelangelo**

1. What is Virus?

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it. A computer virus can not outright damage such as deleting or corrupting computer files. Many people use the term loosely to cover any sort of program that tries to hide its malicious function and tries to spread onto as many computers as possible. Viruses can be very dangerous. For example, a virus that stops a computer and displays a message, in the context of a hospital life-support computer could be fatal. Generally, there are two types of viruses.

1. The first one is file infectors, which attach themselves to ordinary program files. File infectors are again two types:

a. Direct action virus: A direct-action virus selects one or more other programs of a computer to infect each time. The program that contains it is executed. The Vienna virus is an example of a direct-action virus.

b. Resident Virus: A resident virus hides itself somewhere in memory. The first time an infected program is executed, and thereafter infects other programs when they are executed or when certain other conditions are fulfilled. Most of the viruses are resident.

2. The second category virus is system or boot-record infectors. Those viruses that infect executable code found in certain system areas on a disk, which are not ordinary files. Such viruses are always resident viruses.

A few viruses (Tequila virus) are able to infect both direct-action virus and resident virus. These are often called Multi-partite viruses.

There is another virus called Boot-and-file virus. File system or cluster viruses are those that modify directory table entries. So this virus is loaded and executed before infecting the desired program. The program itself is not physically altered. Only the directory entry is altered. Some consider these infectors to be a third category of viruses, while others consider them to be a sub-category of the file infectors.

2. Kinds of Virus

a. Stealth virus
b. Polymorphic virus
c. Fast and slow infectors
d. Sparse infector
e. Companion virus
f. Armored virus
g. Virus hoax

a. Stealth virus: A stealth virus hides the modifications it has made in the file or boot record. Usually by monitoring the system functions used by programs to read files or physical blocks from storage media, and forging the results of such system functions so that programs which try to read these areas see the original uninfected form of the file instead of the actual infected form. Thus the viral modifications go

undetected by anti-viral programs. However, in order to do this, the virus must be resident in memory when the anti-viral program is executed. The very first DOS virus, Brain, a boot-sector infector, monitors physical disk I/O and re-directs any attempt to read a Brain-infected boot sector to the disk area where the original boot sector is stored. The next viruses to use this technique were the file infectors Number of the Beast and Frodo.

b. Polymorphic virus: A polymorphic virus produces varied copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus. The most sophisticated form of polymorphism discovered so far is the MtE (Mutation Engine) written by the Bulgarian virus writer who calls himself the Dark Avenger.

c. Fast and slow infectors: A typical file infector (Jerusalem virus) copies itself to memory when a program infected by it is executed. Then it infects other programs when they are executed. A fast infector is a virus, when it is active in memory, infects not only programs which are executed, but also those which are merely opened. The result is that if such a virus is in memory, running a scanner or integrity checker can result in all programs becoming infected all at once. The term Slow Infector is sometimes used for a virus. If it is active in memory, infects only files as they are modified or created. The purpose is to fool people who use integrity checkers into thinking that the modification reported by the integrity checker is due solely to legitimate reasons. Darth Vader virus is an example.

d. Sparse infector: The term Sparse Infector is sometimes given to a virus that infects only occasionally, e.g. every 10th executed file, or only files whose lengths fall within a narrow range, etc. By infecting less often, such viruses try to minimize the probability of being discovered by the user.

e. Companion virus: A companion virus is one that, instead of modifying an existing file, creates a new program, which gets executed by the command-line interpreter instead of the intended program. This is done by creating an infected .COM file with the same name as an existing .EXE file. Note that this type of malicious code is not always considered to be a virus, since it does not modify existing files.

f. Armored virus: An armored virus is one that uses special tricks to make the tracing, disassembling and understanding of its code more difficult. A good example is the Whale virus. Macro virus many applications allow to create macros. A macro is a series of commands to perform an application-specific task. Those commands can be stored as a series of keystrokes, or in a special macro language. A macro virus is a virus that propagates through only one type of program, usually either Microsoft Word or Microsoft Excel. It can do this because these types of programs contain auto open macros, which automatically run when open a document or a spreadsheet. Along with infecting auto open macros, the macro virus infects the global macro template, which is executed anytime run the program. Thus, once global macro template is infected, any file opens after that becomes infected and the virus spreads.

g. Virus hoax: A virus hoax generally appears as an email message that describes a particular virus that does not exist. These emails almost always carry the same basic story: that if an email downloads with a particular subject line, the hard drive will be erased. Such messages are designed to panic computer users. The writer or writers email the warning and include a plea for the reader to forward it to others. The message then acts much like a chain letter, propagating throughout the Internet as individuals receive it and then innocently forward it. An example of a virus hoax is the "Good Times" virus, which was written in 1994 and since then has circled the globe many times. The best thing to do on receipt of such an email is to ignore and delete it.

3. World Famous Virus Incidents Since 1998:

1. Melissa
2. ExploreZip
3. Chernobyl
4. VBS_LOVELETTER
5. Pakistani Brain
6. Stoned-Marijuana
7. Jerusalem
8. Cascade

9. Michelangelo

1. Melissa: Melissa virus set a benchmark the world over when it was first noticed on 26th March 1999. It was the fastest spreading virus. The Melissa virus is an automatic spamming virus. Its action includes infecting Microsoft Word's normal. Dot global template, basically implies that all new documents created by the user would get infected. After that, each time that an infected document is accessed the virus will disable Microsoft Word's macro warning feature so that it is allowed to be activated.

Its next action is to access Microsoft Outlook address book and e-mail the infected Word file as an attachment to the first fifty e-mail addresses entered there. As soon as the receivers of such an e-mail message open the attachment their computers also get infected. The virus then sends the infected file to another 50 e-mail addresses. This is the reason for the extensive spread of the virus in a short while. The virus by itself, installed in the victim's computer, was rather harmless. It merely inserted some text into a document at a specified time of the day. What caused the maximum harm was that the volume of traffic, due to the numerous e-mail attachments being sent, was more than could be borne by most servers around the world.

2. ExploreZip: The activities of ExploreZip were similar to Melissa. But there was one major difference. ExploreZip, first discovered in June 1999, was not a virus. It was a Trojan. This means that it was incapable of replicating itself. Thus, the Melissa virus had more far reaching presence. In addition to this dissimilarity, ExploreZip was more active. It not only hijacked Microsoft Outlook but also selected certain files and made their file size zero - reduced their data to nothing. Those files were then of no use to the user and they could not be recovered.

3. Chernobyl: Chernobyl, or PE CIH, virus activates itself every year on the 26th of April - on the anniversary of the Chernobyl, Ukraine nuclear power plant tragedy. It was allegedly written by a Taiwanese citizen in 1998. The virus wipes the first megabyte of data from the hard disk of a personal computer thus making the rest of the files of no use. In addition to this it also deletes the data on

the computer's Basic Input-Output System (BIOS) chip so that the computer cannot function till a new chip is fitted or the data on the old one is restored. Fortunately only those BIOSes, which can be changed or updated, face a threat from this virus. This virus affects only executable files. Since these are distributed less often than documents, the spread of Chernobyl is more confined than that of most macro viruses.

4. VBS_LOVELETTER: The VBS_LOVELETTER virus (known as Love Bug or ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus beat the Melissa virus hollow. It became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion.

The original VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail which was sent out had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me". In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user.

Unlike the Melissa virus this virus does have a destructive effect. Whereas the Melissa, once installed, merely inserts some text into the affected documents at a particular instant during the day, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing versions of itself.

5. Pakistani Brain: The Brain, the first virus known to have spread all over the world, was a boot sector virus. This implies that it would take the system commands, those that help in starting the

computer, from their designated space sector on the hard disk and put them in the next unused space sector. Then, it would mark the space where the system commands now reside as bad sectors. This way, it would become impossible to boot (start) the computer. Moreover, it would continue to take up all the unused space in the computer's disk and mark it as corrupted sectors. All the strains of the Brain virus carried the name of the program, the author and often their address in the boot sector of the virus-infected disk become corrupted. The other known versions of this virus include Ashar or Ashar-Shoe viruses, which are very common in Malaysia.

6. Stoned-Marijuana: Stoned-Marijuana virus originally reported to have been written in New Zealand. This was another boot sector virus with a difference. It would infect the boot sector of floppy disks. The File Allocation Table (FAT) on the hard disk drive - the system used by DOS to identify and locate files on a disk - would also be affected. The virus would most often regularly display a message, which said, "Your PC is stoned. Legalize Marijuana." Moreover, it would damage the File Allocation Table on hard disk drives with more than one partition. The FAT on floppy disks, which had been formatted as high density, would also be harmed so that access to files on both the hard disk and the floppy disk would become nearly impossible to achieve.

7. Jerusalem: The Jerusalem virus a.k.a. "Israeli" and "Friday the 13th" has several versions including the Jerusalem-B virus. It starts by infecting the .COM and .EXE files in a computer. After existing or being resident in a computer for half an hour, it slows down the system processes by a factor of ten. On a pre-set date, Friday the 13th, the Jerusalem virus deletes all the infected files from the user's computer. Apart from the damage that it does, the other strain of the Jerusalem virus, Jerusalem-B, also shows a "black window" in the center of the screen at regular intervals.

8. Cascade: The Cascade virus originally appeared between September and December during the years 1980 and 1988. Its basic target was machines with color monitors. This virus is also called "Falling Letters" or "1701". It initially appeared as a Trojan horse in the

form of a program designed to turn off the Num-Lock light on the user's keyboard. It actually makes the characters on the screen drop in a heap to the bottom of the screen. The specialty of this virus is to utilize an encryption algorithm to evade detection. Now, variants of this virus occur as a memory resident .COM virus.

9. Michelangelo: The Michelangelo virus also referred to by some virus watchers as Stoned. Michelangelo, first spread in the early 1990's. Since then, a number of strains have been introduced, and it is now also known by a variety of other names. This virus was also responsible for the founder of Trend Micro entering the anti-virus business.

This virus was entitled after the very famous Italian Renaissance artist Michelangelo Buonarroti. It gets activated every year on the artist's birthday - 6th March. The person responsible for giving the name was the researcher not the writer of the virus.

The Michelangelo is a boot record virus and on the date that it gets triggered it destroys files by overwriting certain critical areas of the hard disk or floppy disk. These areas are overwritten with garbage, making the disk or floppy completely useless. If this virus infects a bootable floppy (a floppy that can be used to boot a computer), the floppy no longer remains a bootable floppy.

An infection with this virus is caused by using infected disks for a system boot-up. After being installed in the memory of the computer, Michelangelo then goes on to infect all non-write protected disks that are used in the computer.

Chapter–12
Worms

1. What is worm?
2. History of Worms
3. World Famous Worms
- **a. The Christmas tree Worm - 1987**
- **b. The Internet Worm - 1988**
- **c. The SPAN network worm – 1989**

1. What is worm?

A computer worm is a self-contained program that is able to spread functional copies of itself or its segments to other computer systems usually via network connections. Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms

1. Host computer worms
2. Network worms.

1. Host computer worms: Host computer worms are entirely contained in the computer. It runs on network. It uses network connections only to copy themselves to other computers. A host computer worms terminates it after launching a copy on another host computer. These are called rabbits.

2. Network worms: A network worms consist of multiple parts called segments. This network worms is running on different machines and perform different actions on the network. It uses the network for several communication purposes. For Example propagating a segment from one machine to another is one of those purposes. Network worms have one main segment, which coordinates the work of the other segments. These are called octopuses.

2. History of Worms:

The term worm was used for the first time by science fiction author John Brunner in his book called 'The Shockwave Rider'. Brunner described a totalitarian form of Government, which would keep a

control over their citizens by the use of a powerful computer network. In this story a freedom fighter was introduced into this computer network system for contamination. This was called a Tapeworm. This tapeworm harassed the system and forced the government to shut down the network. As a result their main base of power was lost.

The first worms in history were actually designed to do well and not to do harm to networks. The first worm was developed for the assistance of air traffic controllers by Bob Thomas in 1971. This worm notifies air traffic controllers when the controls of a plane moved from one computer to another. This worm is called Creeper. It would travel from one computer screen to the other on the network showing the message, "I'm Creeper, Catch me if you can?" These creepers could not be able to reproduce it. This is the character of the creepers and the difference between the creepers and the other worms.

This idea of developing worms was slowly faded out away. A few people did try to experiment with this worm. John Shock and Jon Hepps of Xerox's Palo Alto Research Center was the pioneer of this work. In the early 1980s they began working on worm programs. This was also the first time that this type of program was called a worm.

Both of them developed total 5 worms. These were specially designed to perform a particular function. They were programmed to do certain tasks around the network. The simplest of these worms was a 'town crier' worm. Its job was only to post announcements on all the computers of the network.

The more complicated worms was developed which would remain completely dormant during the day and would activate only in the night. Once all the employees had left for the day, this worm would harness the extra computing power of the idle computers to do tasks which required more computing power. In the morning, before the arrival of the employees it would save all the work done during the night and become dormant till the next evening.

Although these programs were apparently helpful around the network, their developers were given a rude glimpse of their inherent

destructive possibilities. One morning when the employees returned and find that all the computers had crashed. When they tried to restart the computers, they crashed again. It was found that one of the worms had malfunctioned and had created havoc in the network. A vaccine had to be created so as to deactivate the worm before the computers on the network could become functional again.

3. World Famous Worms: There are three famous worms-

a. The Christmas tree Worm - 1987

b. The Internet Worm - 1988

c. The SPAN network worm – 1989

a. The Christmas tree Worm - 1987: The Christmas tree worm was a combination of a Trojan horse and a chain letter. This was a mainframe worm and managed to paralyze the IBM network on. The Christmas day 1987 worm was written in a language called Exec. It asked the user to type the word 'Christmas' on the screen. Then it drew a Christmas tree and sent itself to all the names of people stored in the user files 'Names' and 'Netlog' and in this way propagating itself.

b. The Internet Worm - 1988: On November 22, 1988, Robert Morris, a Cornell University science graduate accidentally released his worm on a very large network in the area. This network was named Arpanet, which later went on to become the Internet. The worm managed to infect approximately three thousand computers during eight hours of activity. The Internet worm as it came to be known disabled all those machines by making copies of itself and thus clogging them. Apart from clogging all the security loopholes, many machines had to be completely taken off the network till all copies of the worm could be totally removed. Although the entire process took the scientists almost two to three days, no data was lost on any of the infected computers and no permanent damage was done to any of the computers.

c. The SPAN network worm - 1989: On the October 16, 1989, a worm named WANK infected many VAX and VMS computers

on the SPAN network. This worm, if it found that it had system privileges, would then change the system announcement message to 'Worms against Nuclear Killers'. The message was then graphically displayed as the first letters of each word and the last three letters of the last word.

Chapter–13
Trojans

---

1. What is Trojans?

In the 12th century BC, Greece declared war on the city of Troy. The dispute erupted when the prince of Troy abducted the queen of Sparta and declared that he wanted to make her his wife. This naturally angered the Greeks and especially the queen of Sparta. The Greeks besieged Troy for 10 years but met with no success as Troy was very well fortified. In a last effort, the Greek army pretended to be retreating, and left behind a huge wooden horse.

The people of Troy saw the horse. They thought that these were some kind of a present from the Greeks. They pulled the horse into their city. But they did not know that the hollow wooden horse had some of the best Greek soldiers sitting inside it. At night the soldiers came out and opened the gates of the city. These soldiers together with the rest of the Greek army fought and killed the entire army of Troy.

Trojan is a kind of computer program. It is similar to the wooden horse. A Trojan horse program pretends to do one thing while actually it is doing something completely different.

2. Types of Trojans

a. Remote Administration Trojans (RATs)
b. Password Trojans
c. Privileges-Elevating Trojans
d. Key loggers
e. Destructive Trojans
f. Joke Programs

a. Remote administration Trojans (RATs): Remote administration Trojans (RATs) are the most popular Trojans. They let a hacker to access into the victim's hard disk. It perform many functions on victims computer like shut down computer, open and close his CD-ROM drive etc. Modern RATs are very simple to use. These come packaged with two files. These are -

(1) the server file and

(2) the client file.

The hacker tricks someone into running the server file, gets his IP address and gets full control over his/her computer. Some Trojans are made limited by their functions. Some Trojans are merely meant for the attacker to use them to upload another Trojan to his target's computer. Hackers also bind Trojans into other programs, which appear to be legitimate. For example a RAT could be bound with an e-greeting card. Most RATs are used for malicious purposes.

There are many programs that detect common Trojans. Firewalls and anti-virus software can be useful in tracing RATs. Remote administration Trojans (RATs) opens a port on the computer and binds themselves to it. While someone runs his client program on the computer, RATs enters into the victim's IP address. Then the Trojan starts receiving commands from the attacker and runs them on the victim's computer.

b. Password Trojans: Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. The Passwords may be Internet password or an email password. There is a Trojan which used for every password. These Trojans usually send the information back to the attacker via Email.

c. Privileges-Elevating Trojans: Privileges-Elevating Trojans are usually used to make system administrators fool. They can either be bound into a common system utility or pretend to be something harmless. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileges users and give the attacker access to their account.

d. Key loggers: Key loggers **Trojans** are very simple. They log all of the victim's keystrokes on the keyboard including passwords. Then they either save them on a file or email them to the attacker. Key loggers usually don't take much disk space and can masquerade as important utilities, thus making them very hard to detect.

e. Destructive Trojans: Destructive Trojans can destroy the victim's entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually ripping every file they encounter to pieces.

f. Joke Programs Trojans: Joke programs Trojans are not harmful. They can either pretend to be formatting hard drive, sending all of passwords to some hacker, self destructing computer, turning in all information about illegal and pirated software might have on computer to the police or to Privacy Watch etc. In reality these programs do not do any thing harmful.

3. Some common Trojans are as follows:

a. Back Orifice (BO)
b. NetBus
c. NetBus 2 Pro
d. D. Deep throat v 2

a. Back Orifice (BO): Back Orifice (BO) Trojan was developed by a community of hackers known as 'Cult of the dead cow' (www.cultdeadcow.com). This Trojan can be downloaded from www.BO2K.com and numerous other websites. Back Orifice consists of two parts, (1) a client application and (2) a server application (approximately 122 KB). The client application, running on the hacker's computer, can be used to monitor and control the victim's computer which runs the server application.

b. NetBus: NetBus was developed by a Swedish citizen named Carl-Fredrik Neikter who claimed that he developed it purely for fun.

Netbus can be downloaded from hundreds of websites. It is best to use Google.com to search for the program. Netbus allows the hacker to do numerous activities on the victim's computer.

c. NetBus 2 Pro: NetBus 2 Pro is the legitimate version of NetBus. It affects computers running the Windows 95, 98 and NT operating systems. The server portion (named "NBSvr.exe") is approximately 599 KB in size. Once installed NetBus is run every time the computer is started. Carl-Fredrik Neikter who is also the creator of the original NetBus developed NetBus 2 Pro.

d. Deep Throat v 2 : Deep Throat was developed by a person called ^Cold^ Killer, CEO of DarkLIGHT Corp. Deep Throat v 2 affects computers running the Windows 95 , 98 operating systems. The Trojan deletes the existing 'systray.exe' file of the victim computer (which is normally 36 KB in size) and replaces it with the 'server' portion of the Trojan (which is approximately 301kb in size). Once installed, it runs every time the computer is started. Among other things, Deep Throat allows the hacker to open / close the CD-ROM tray of the victim's computer, restart the victim computer, get a screen dump, and start an FTP Server on Port 21 of the victim.

Chapter–14

Cyber Forensics and Investigation

1. **What is Cyber Forensics?**
2. **Cyber Crime Investigation Process**
3. **Some case reference on Cyber forensics**
4. **Preservation of Electronic Records in a court of Law**
5. **Digital Evidence Searching Process**

---

1. What is Cyber forensics?

Cyber forensics is belonging to courts of law. It includes computer forensics and network forensics. Cyber forensics is involved in finding password protected information, encrypted information and contents. It also work for tracing the source of E-mail, Tracking software piracy, recovering deleted data, matching information, remotely monitoring computer and preserving digital evident to present in the court.

2. Cyber Crime Investigation Process:

At the time of cyber crime investigation the collected information and the physical items may acquisitioned as digital evidence. Proper measure should be taken to protect the original digital evidence. For this a duplicate copy of the original digital evidence should be taken.

Original digital evidence includes the physical items and the related electronic data. During acquisition digital evidence should be kept secured and protected. Duplicate digital evidence is the accurate digital reproduction of all electronic records contained on an original physical item and this duplicate digital evidence should be used for investigation.

Examination of a computer to discover data is stored on it is time consuming and painstaking process. Proper and through examination is very important. A computer stored many types of information. These are valuable from the evidence point of view. These are normal files, deleted files, password protected information, hidden file, data in free space, file slack, RAM slack, driye slack space, and unallocated space.

The original computer should be treated with great care. It must not altered by any examination process. Because this may be infected by viruses, logic bombs, booby traps, worm, Trojans etc and may alter the data contained in the original computer.

At the time of examination the original evidence generally not used. The investigator at first makes an image copy of all the data of the original computer and then examines this copy and thus original evidence remains in initial forms. This process ensures that tempering of the original evidence does not occur. This mirror image is known as a bit-stream image. Bit-stream image can provide all the information about stack created in the various files, the unallocated storage space to the investigator with the data or information stored there. This method ensures that the original evidence is not tempered with.

3. Some case reference on Cyber forensics

1. A USA Court in Northwest Airlines et al v. Local 200 el al, CA No. 00-08DWF/AJB(D.Minn. 2000) (Case settled without trial) was directing the plaintiff's expert to make mirror images of the drives on the defendant's computer. The original drive were not released but were entered as evidence.

2. In Gates Rubber Co. v. Bando Chemical Industry Ltd. 167 F.R.D. 90 (D. Colo 1996) A USA court ordered investigation of some computerized files. Due to miss handling of the evidence, the court then passed a stricture on one of the parties for not having made an image copy of the drive at the outset. The Court ruled that while collective evidence for judicial purposes the investigating party had a duty to utilize the method which would yield the most complete and accurate results. USA court recognized the need, importance and value of the Cyber forensics.

3. In Easley McCaleb & Assocs. Inc v. Perry, No. E-2663(Ga. Super. Ct. July 13, 1994) the court held that deleted files on a defendant's computer hard disc drive are discoverable and the plaintiff's expert must be allowed to retrieve all reasonable files. In this case the defendant of his own volition had deposited the hard disc drive in question into the registry of the court. The plaintiff moved for discovery of its contents, including files that had been deleted where they could be recovered. The court guaranteed defendants motion and issued an order detailing the procedures for reviewing electronically stored for both parties.

4. In Strasser v. Yalamanchi 669, So. 2d. 1142 (Fla Dist. Ct. App. 1996) the court held that it might order on-site inspection of computer hardware to recover purged records. Such order could be made upon a

showing that relevant discoverable evidence may be recovered and that adequate measures would be taken to protect privileged data.

5. In Playboy Enterprises Inc v. Terri Wells, 60 F. Supp. 2d. 1050 (S.D. Cal. 1999) the court held that the routine deletion of E-mail does not render the E-mail undiscoverable if it can reasonably be recovered. The court held that it had the power to appoint a natural computer expert to recover the E-mails.

4. Preservation of Electronic Records in a court of Law

Cyber forensics produces Electronic records in a court of law. So it is important to attached Electronic records by the judiciary. Some references are given below:

1. In 1973 American Courts were cognizant of the fact that computerized record keeping were rapidly becoming a normal procedure in the business world.

2. Section 2(1)(t) of The (Indian) Technology Act 2000 defines an Electronic Record as data or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

3. The electronic Signature in Global and National Commerce Act of the USA states the term Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Also in United States Rule 201 of the Illinois Supreme Court defines the word Documents as including all retrievable information in computer storage.

4. Canada's Uniform Electronic Evidence Act defines key terms, such as Electronic Record and Electronic Record System and provides a series of rules and presumption relating to the admissibility of electronic records. A presumption of integrity is given to electronic records when it is established that

(a) at all material times the computer system was operating properly or the fact it was not operating properly or the fact that it was not operating properly did not affect the integrity of the electronic record and

(b) there are no reasonable grounds to doubt the integrity of the electronic records system.

5. **In Crown Life Insurance Co. V. Craig, an American Court** held that data from a computer data base is a Document within the meaning of the Federal Rules of Civil Procedure and must be produced in accessible form. This view was retreated in another American case Anti Monopoly, Inc. v. Hasbro Inc.

Relevant US Case Laws: USA Judgments have emphasized the value of electronic records as evidence.

1. **In Armstrong v. Executive office of the President,** 821F. Supp. 761, (D.D.C.1993) the court held that Government E-mail is a record as defined by the Federal Record Act and that it was insufficient for the Government to preserve only the paper printout of such message.

2. **In Timken Co. v. United States,** 239(Ct. Int'l Trade 1987) the court ordered, production of data on computer tape even through it had been produced in paper prints

3. **In Public Citizen Inc. v. Carlin,** 2DL.1 (D.D.C. Oct. 22 1997)(Carlin 1) overruled bg 1184 F 3rd 900 D.C. Cir. August 6,'99 (Carlin 2) the court found that US Government policy of destroying electronic document after printing them a "arbitrary and capricious." The court acknowledge electronic documents are unique and distinct from printed versions of the same records and of grater utility that their paper printout.

4. **In the case of Adams v. Dan River Mills Inc.** 54 F.R.D. 459, 462 (D.Uth 1985) the court held that discovery of information stored in new and different media, including purchased data cards, computer tapes, floppy and hard disks and computer memories, even though not as easily accused as the traditional tangible forms of information storage (paper), is nevertheless both necessary and proper.

5. **In Anti-Monopoly Inc., v. Hasbro Inc.** 94 CIV.2120, 1995, U.S. Dist. Lexis 16355 (S.D.N.Y. 1995) the court stated that "today it is black letter law that computerized data is discoverable if relevant", which in Bills v. Kennecott, 108 F.R.D. 459, 462 (D.Utah 1985) it was held that "computers have become so commonplace that most court battles now involve discovery of some type of computer –stored information.

6. **In Crown Life Insurance Company v. Kerry P.Craig** US Court of Appeal; 7th Circuit #92-3180. the court rejected an arrangement that "written documents" referred only to documents in hard copy (on paper) form.

7. **In Greyhound Computer Corp. Inc., v. IBM,** 3 Computer L. Serv. Ref. 138, 139, (D.Minn. 1971) it was held that information provided must be in a "reasonably unable form" and courts will ensure that the party requesting the information is able to access the data. In this case the dependant provided computer tapes that plaintiff was unable to read, court ordered dependant provided computer tapes that plaintiff was unable to read, court ordered dependant to assist the plaintiff accessing the information with materials and personnel.

8. **In International Business Machines v. Comdisco Inc.** 91. 6-67-194, 1992, Del. Super LEXIS 67 Mar. 11, 1992, it was held that attorney client privilege can extend to computer files. Counsel's advice or opinion was conveyed through electronic mail, then that message is privileged. Court said it was privileged "except to the extent that it contains information meant to be obtained to persons other then the corporate client."

9. **In Monotype Corporation Plc. V. International Typeface Corp.** 41 F.R. Evid. Serv. 86(9th Cir. 1994, the court found that E-mail, being merely an ongoing electronic measures and retrieval System" is far less a 'Systematic' business actively than are record-keeping computer printouts.

10. **In US v. Kim** , 595, F-2d, 755(D.C. air 1979) discussing the admissibility of a telex, the court explained that the "critical factor in determining whether the documents satisfied the business purpose requirement lies in the reason that the message was prepared and sent not the means by which it was transmitted."

11. **In National Union Electric Corp. v. Matsushita Electronic Industries Co.** 494 Federal Supp. 1257, & 126 it was held that the manufacturer of machine readable copy of a computer disk is in principle, no different form the manufacturer or photocopy of a written document. The court went on to observe "we now live in a society when much of data which our society desire in stored in computer disk. This process will escalate in years to come, we suspect that by the year 2000virtually all data be stored in some form of computer memory."

12. **In Santiago v. Mills,** the court noted that 'A request for new information in computer Bank is proper and the information is

obtainable under the discovery rules. In **US v. Catabran,** 121 F.R.D 636, 640, (W.D.N.Y.) 1988) 836 F. 2d. 453. (9th Cir.1988) that court held that computerized printouts of accounting and other booking keeping records are admissible as business records.

5. **Digital Evidence Searching Process:** (Details given in chapter 15, Digital Evidence)

The followings are the digital evidence searching Process:

a. Target Definition
b. Search Process
c. Crime Scene Data Processing Phase
d. Data Comparison Phase
e. Automation
f. Target Definition Based on Existing Evidence
g. Digital Storage of Target Objects
h. Target Object Suggestions
i. Parent Directory
j. Similar Name
k. Name in Content
l. Temporal Data
m. Application Type

Searching for digital evidence is a time consuming and error-prone process. Introducing techniques to automate the searching process could make helpful. Data mining techniques can also be used to find files and directories created during the incident. The data mining techniques detect a higher percentage of files than a random sampling would, but there are still many false positives. More research into the error rates of manual searches is needed to fully understand the impact of automated techniques.

Chapter–15
Digital Evidence/E-Evidence

1. What is Digital Evidence?

The term digital evidence encompasses any and all digital data that can establish that a crime has been committed. With the rapid development of electronic commerce and Internet technology, cyber crimes have become more and more common. There is a great need for automated software systems that can assist law enforcement agencies in cyber crime evidence collection. For example DESK (Digital Evidence Search Kit) is an effective cyber crime evidence collection tool.

The legal rules regulating the search warrant process must be revised in the light of the demands of digital evidence collection. Present existing rules permitted one-step process of traditional searches and seizures. That is the police obtain a warrant to enter the place to be searched and retrieve the property named in the warrant. Computer technologies are tend to bifurcate the process into two steps:

1. The police first execute a physical search to seize computer hardware,
2. Later execute a second electronic search to obtain the data from the seized computer storage device.

So the Digital evidence is the process of proofing Cyber crime of the present computer world.

2. Recovery of Digital Evidence:

Every cyber crime has certain unique points. These determine the initial steps to be taken towards the recovery of digital evidence during investigation of the crime. Once these initial procedures have been completed the actual process of data recovery can begin. It is important in a court that the examination has been conducted thoroughly and the evidence is authentic and unaltered.

3. Hard disk examination:

The procedures to be followed for examining hard disks

1. The media used for examination process, should be virus free.
2. The original media should not be used for the examination. A bit-stream image of the original hard disk should be used.
3. The bit-stream image should be verified by MD5 hash value.
4. The boot record data, command files should be examined.
5. All recoverable deleted files should be restored.

6. All the files contained on the hard disk should be listed.
7. The unallocated storage & slack space should be examined.
8. Attempts should be made to decrypt password-protected files.

4. Floppy Disk Examination:

The procedures to be followed for examining floppy disks:

1. The media used for examination process, should be virus free.
2. A duplicate image of the original floppy disk should be made on another floppy disk.
3. A copy of the original floppy disk should be logically examined and all information contained therein should be documented.
4. All recoverable deleted files should be restored.
5. All the files contained on the hard disk should be listed.
6. The unallocated space and slack space should be examined.
7. Attempts should be made to decrypt password-protected files.

5. Types of Files to be examined

Information contained in a computer can be divided into certain predefined types of files. This are-

a. Normal File
b. Deleted files
c. Password protected files
d. Hidden Files
e. Encrypted files
f. File Slack
g. RAM Slack
h. Drive Slack

The ways in which information can be retrieved from files are stated below:

a. Normal Files: These are regular files used by the user and easy to access. Most of the time, users do not encrypt this information and nor do they have any passwords to protect it. These files may contain evidence like incriminating letters, notes, figures, etc.

b. Deleted files: These are the files that have been deleted by the user. Usually when any file is deleted it may be possible to recover it from the Recycle Bin of the computer. If the user has been cautious

last cluster assigned to the file which is called File Slack. To fill in this space randomly selected data from the computer's memory is used. File Slack is created at the time when a file is saved to disk. File slack is created utilizing randomly selected data from the computer memory. Due to this it may contain and assist investigators in identification of network logon names, passwords and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the suspected computer and such legacy data can help the investigator. Fragments of prior email messages and word processing documents can be found in file slack. It potentially contains evidence that may have been thought to be lost.

g. RAM Slack: The data used for padding is taken from the memory buffers of the system. This data originates from the memory of the computer is called RAM Slack. RAM slack pertains only to the last sector of a file. RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during the past work sessions since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past. Such information could help investigators gather evidence of the files on which a suspect may have worked.

h. Drive Slack: In certain situations, more or additional sectors need to be added to fill out the blocks of the last cluster assigned to a particular file. In such a case, a different kind of slack has to be created. This is known as Drive Slack. This is then stored in the sectors needed to fill up the last cluster for a file. Drive Slack contains data from what was previously stored on that particular storage device. The data or information contained in the Drive Slack is derived from the format pattern associated with disk storage space. The perpetrator of the crime may assume these files to be completely deleted or wiped out. But these may be procured from the Drive Slack.

6. Investigation and Recovery of information from the browser:

Another good place to retrieve information is the user's cache memory. The URL line at the top of the browser contains a drop-down list box of recently visited sites and will auto-complete. As a user selects a URL or types one partially in, the past URLs visited by the user also appear. Most browsers keep a list of all the URLs that a user

has browsed. A few clicks of the button will open this list. Even deleting the cache doesn't always get rid of the files. There are many ways to recover these lost files. This are-

1. The first step would be built in undelete programs.

2. The next would be disk scanners which disregard directory entries and pull data directly from the disk.

3. A third method can sometimes recover overwritten files.

When things are overwritten, magnetic traces of the original data are left behind on the disk. This is why it is recommended that free space should be overwritten at least 7 times in order to completely erase old data. Such wipe features come as part of many encryption packages.

Most sites drop cookies on machine. By opening the cookie list the investigator can see all the cookies deposited there. Most users are not even aware of the existence of cookies so an investigator who knows about them may be able to discover many of the sites accessed by the user. The same methods of data recovery can then be applied to the retrieval of information from removable storage media like floppy disks, CD-ROMS, Zip Drive, etc.

In certain cases, the complete examination of all the computers on a network becomes redundant. If the machine used to commit a crime is a stand-alone machine then all the forensic procedures and examination can be conducted only on that machine. This concept is known as limited examination. It depends upon the investigator to decide what kind of examination will need to be conducted.

The other part of the investigation involves regular forensic procedures and regulations to be followed. Investigators have to take the statements of the computer users, witnesses, etc. These statements have to give details of the usage of the machines.

Finally, it is extremely necessary that the authenticity of all the evidence can be proven in a court of law. So we can reiterate here that each step taken by the examiners should be documented in detail.

7. Investigation and Examination of log files:

Computers maintain important information in log files. Such files are generated by web servers, FTP servers, email servers, firewalls and even modems. Web servers store important information in files with the log extension. These files can be opened as text files to read the raw log data.

b. Search Process: The search phase of a digital investigation is the digital crime scene. It is processed and evidence is recognized. The primary goal of this phase is to recognize objects that played a role in events related to either the incident or a hypothesis about the incident. The evidence searching should verify an incident report, to find evidence of a specific event, or to test a hypothesis. Keyword search defines a digital representation of the target object. Target objects are defined based on incident hypotheses. It is one of the most challenging phases of the search process.

c. Crime Scene Data Processing Phase: The searching process is to process the crime scene data objects. The format is needed to compare them with the target object characteristics. The amount of processing needed depends on -

a. The type of data collected from the crime scene,

b. The characteristics that have been defined in the target object,

c. The amount of crime scene data preprocessing that was performed.

During the search, data are processed in some pattern. At physical crime scenes, the physical objects are examined as they are seen by an investigator who is walking around in geometric patterns.

d. Data Comparison Phase: The searching process compares with followings-

1. The processed crime scene data object characteristics and
2. The target objects characteristics.

If they match then it can consider the crime scene data object to be evidence. Comparisons can be done-

1. Automated,
2. Manual, or
3. Combination of both.

Manual comparisons are performed using visual techniques. The data are displayed to the investigator and compares them with the target object. Fully automated comparisons are rare. Fully automated comparisons can be used for simple targets. The target object is fully represented in a digital format. The combination of automated and manual comparisons is more common. The target object will be partially defined in a digital form and the search tool will locate objects that match the digitally defined characteristics and list them. The

investigator visually compares the listed objects to the target characteristics that were not digitally represented.

e. Automation: It is clear that some data comparison phases will be benefited more from automation. The Data Comparison Phase can be easily automated if the target object is digitally defined. The Automated Target Definition Phase has the benefit of having a digital target object. This can help in the automation of the Data Comparison Phase.

f. Evidence Based on Target Definition: The basic concept of the investigator is to uses an analysis tool to identify files as evidence Based on Target Definition. The tool makes suggestions for additional searches. This is an intuitive step performed by the investigators. They are designed to analyze a bitwise copy of a hard disk or partition, called an image file. There were two major features that needed to be added to Autopsy for the automated searching. These are -

1. Method for storing the target objects to be used later,
2. The process of suggesting new target objects

g. Digital Storage of Target Objects: The first new addition to personal inspection is the digital representation and digital storage of target objects. The concept of implementation depends on seven characteristics of the target objects. These are

1. Parent Directory Name
2. File Name
3. Last Modified (or Written) Time
4. Last Accessed Time
5. Last Changed (or Created) Time
6. Application Type
7. Content Keyword

After a target object has been defined, an investigator can conduct the search by selecting the target from a list. If the file or directory name fields were defined in the target, then a file name search pattern is used and the search hits are listed so that the investigator can view the contents and metadata information for each. If the file content is used in the target, then a keyword search is conducted in each data unit. If the application type was defined in the target, then personal investigation will show a list of files that have the same application. If the time field was defined in the target object, then the timeline view of the file system is used to show the files that had activity at that time.

h. Target Object Suggestions: The second addition to Personal inspection was a process to suggest new target definitions based on the characteristics of recently found Evidence. The original version of Personal inspection had a feature to create a note, similar to a bookmark, about data. In the updated version, the window that allows the investigator to make notes also provides a list of additional searches that could be relevant. The investigator can choose to save or ignore the suggestions. The basic approach uses several static algorithms for suggesting new targets. The user has the choice of editing the target objects before saving them. If the new evidence was a file, then up to seven default target objects are suggested. If the suggestion has already been made, then it will not be shown again.

i. Parent Directory: The target object has the Parent Directory Name attribute defined with the same name as the parent directory of the evidence. This is useful when a file is found because of a keyword and the surrounding files have not yet been examined.

j. Similar Name: The target object has the File Name attribute defined with the same name as the evidence. The investigator can remove the extension or other parts of the name so that files with similar names or extensions can be found. This is useful to find configuration files that have a different extension or to find duplicate copies of the file.

k. Name in Content: The target object has the Content Keyword attribute defined with the name of the evidence file. This will find files that reference the evidence file and have not used any obfuscation techniques.

Temporal Data: Up to three target objects are created and each has one of the Last Modified or Written, Last Accessed, or Last Changed or Created values defined. This can be used to find other files that played a role in events in the same time frame as the evidence.

Application Type: The target object has the Application Type attribute defined with the same type as the evidence file. This can be used to find additional files of the same type. The investigator is also given the strings from the file content and she can create additional target objects based on them. For example, a target object's File Name or Content Keyword characteristics can be defined using data in the evidence file's content. Future work will work on techniques to suggest searches based on the content. While the suggested searches are all

intuitive, the unique aspect is that the investigator is reminded of the additional searches that could be useful. These are saved so that the investigator does not forget to conduct them.

l. Single Attribute File Outlier Detection

A second method of automatic target definition uses outlier analysis to find files that have been hidden or that are different from their surrounding files. The motivation for this target definition technique is that it is common for new files to be created during an incident the attacker typically takes steps to hide these files from detection. Outlier analysis may be able to detect these hidden files. One method is to place them in a directory that already has many files and the theory is that they will not be noticed by casual observation. The files to be hidden are given names similar to existing files and the temporal data are changed. The files hidden using these methods will likely have different characteristics from their surrounding files.

m. Multiple Attribute File Outlier Detection:

To reduce the number of false positives that was found using single attribute outlier analysis. Multiple attribute outlier analysis uses two or more attributes for each point to detect outliers. The motivation for using multiple attributes was that some of the false positives occurred because one of the file's. Attributes was very large or small. On the other hand, it could also reduce the accuracy count because some of the incident files will have only one outlier attribute and therefore not be identified. One of the difficulties when considering multiple attributes of data is how to measure the distance between the points.

9. Investigation related tools:

1. Preservation Tools: Tools that can be used to help preserve the state of a system

2. Tribble: Tribble is a hardware expansion card that can reliably acquire the volatile memory of a live system to removable storage. The hardware device directly accesses memory and does not require software to be loaded, which will overwrite possible evidence.

3. Search Tools: Search Tools that can be used to search for digital evidence

4. Autopsy Forensic Browser: Autopsy Forensic Browser is an HTML-based front-end graphical interface to The Sleuth Kit Autopsy

allows an investigator to examine a file system image from a "file manager" like interface, view unallocated space and data structures, make timelines of file activity, and conduct keyword searches.

5. Mac-robber: Mac-robber is a forensics and incident response program that collects Modified, Access, and Change (MAC) times from files. The output can be used with The Sleuth Kit to create timelines of file activity.

6. The Sleuth Kit: The Sleuth Kit is a collection of UNIX-based command line tools that allow an investigator to view the files and deleted content in NTFS, FAT, FFS, EXT2FS, and EXT3FS file system images. The tools also allow the investigator to perform hash database lookups and sort files based on their structure. The Autopsy browser can be used with TSK to automate many of the functions.

7. TCT-utils: TCT-utils is an add-on to The Coroner's Toolkit that provides file name analysis and mapping between file system layers. It is no longer supported.

10. E-evidence in Bangladesh:

In criminal justice, the Bangladesh legal system follows Evidence Act 1872. As most of the cyber crimes are conventional in nature, the conventional legal systems are to be followed. Accordingly the conventional Evidence Act 1872 should be followed.

The (Indian) Information Technology Act 2000 amends the Evidence Act to meet the necessity of the Cyber Law in respect of evidence. Bangladesh proposed for legislating Bangladesh Information Technology Act which is under active consideration of the Government.

In this Proposed Bangladesh Information Technology Act, necessary provisions has been given in The Second Schedule to amend some sections of the Evidence Act 1872 to make it more effective in respect of Cyber Law and Cyber crime. Some necessary provisions have been included in this proposed Act. So it may be said that Bangladesh is going to update the Evidence Act 1872 as per requirement of Cyber law and cyber crime.

Chapter–16
Cyber Crime Cases

A. Unauthorised Access
B. Email Related
C. Defamation
D. Computer Fraud
E. Pornography
F. Online Gambling
G. Miscellaneous

Internet network make the world very closer to each other. Information is readily available on the cyber space. So the users of the computer network want to be one nation and may be called cyber nation. Computer world do not agree to maintain the geographical territorial limitation. It wants to create a new civilization which may be called cyber civilization.

Cyber crime is a global issue. To control the cyber crime cyber law become essential. Some case references are mentioned here on the following cyber crimes.

A. UNAUTHORISED ACCESS
B. EMAIL RELATED
C. DEFAMATION
D. COMPUTER FRAUD
E. PORNOGRAPHY
F. ONLINE GAMBLING
G. MISCELLANEOUS

A. UNAUTHORISED ACCESS

1. Briggs v. State of Maryland 348 Md. 470 (1998) [USA]

The Court held that the statute of the state of Maryland that criminalizes unauthorized access to computers "was intended to prohibit use of computers by those not authorized to do so in the first place, and may not be used to criminalize the activities of employees who use employers' computer systems beyond the scope of their authority to do so".

2. Scott Moulton and Network Installation Computer Services, Inc. v. VC3 Civ. Act No. 1:00-CV-434-TWT (N.D. Ga.November 6, 2000) [USA]

The Court held that the plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act.

3. Regan Gerard Gilmour v. Director of Public Prosecutions (Commonwealth) No. 60488/95 in the Supreme Court Of New South Wales [Australia]

The accused was a public servant employed as an Administrative Services Officer Grade 3 within the Debt Management Section of the Australian Taxation Office in its Relief Section. The Relief Section considers written applications by taxpayers for relief from payment of income tax.

Upon receipt of an application the Relief Section prepares a submission, which objectively sets out the application and attaches relevant documents but makes no recommendation as to whether or not relief should be granted and the submission is forwarded together with the application to an appropriate person. This appropriate person then determines whether or not relief should be granted.

Following the determination of an application, the accused was required to insert data into a computer system called the Compact Computer System, which operated, only in the Debt Management Section. This data was eventually entered on the taxpayer's general file held by the Australian Tax Office.

The accused had no authority to grant relief. For the purpose of carrying out the duties of his employment, he had access to the computer by entering his user ID and password. His duties included the entry of various codes into the computer. He was permitted by his employer to enter relief code "43" only where relief had been granted.

The computer system had the capacity to be programmed to restrict the insertion of data and to beep and display the words "no right of access" if insertion was attempted contrary to the restriction.

The computer was not so programmed to restrict entry of relief code "43" by the appellant.

In 19 cases no grant of relief had been made and the accused knew this to be the case. Accordingly, the appellant was not permitted by his employer to enter relief code "43" in these cases. However, in all the 19 cases, the accused inserted data, relief code "43", in the computer indicating that relief had been granted when this was not the case. The computer received this data in each case.

There was no financial gain to the accused in taking this course. He did so because of a desire to expedite the process, a heavy workload and concern about suggested inconsistencies in determinations of applications for relief.

The Court was required to determine whether the accused had "authority" to insert data in a Commonwealth computer for the purpose of section 76C of the Crimes Act 1914 when the computer would physically accept his insertion of data, but the accused was not permitted by his employer to insert the relevant data, relief code "43", in the computer without specific permission given by the employer prior to the insertion and such permission was not given in these cases".

As per section 76C of the Crimes Act 1914, "A person who intentionally and without authority or lawful excuse: (a) destroys, erases or alters data (Data" is defined by section 76A as including information, a computer program or part of a computer program) stored in, or inserts data into, a Commonwealth computer..... is guilty of an offence".

The Court held that a person commits an offence under this section if he lacks the authority to insert the particular information into a computer, notwithstanding that he has general authority to insert other information into such computer. The Court further held that an entry intentionally made without lawful excuse and known to be false is made without lawful authority.

4. Director of Public Prosecutions v Murdoch (1993) 1 VR 406 [Australia]

In this case, the court held that section 76 C of the Crimes Act 1914 does not distinguish between what are colloquially known as "hackers". and persons who have some authority of some kind to enter the computer system. Rather the section invites attention to whether the particular entry or gaining access to the computer system was with or without lawful authority.

The Court held that where the question is whether the entry was with permission, it would be important to identify the entry and to determine whether that entry was within the scope of the permission that had been given. If the permission was not subject to some express or implied limitation, which excluded the entry from its scope, then the entry will be with lawful justification but if the permission was subject to an actual express or implied limitation, which excluded the actual entry, made, then the entry will be "without lawful authority to do so".

4. America Online Inc. v. National Health Care Discount, Inc 2000 U.S. Dist. Lexis 17055 (N.D. Iowa, September 29, 2000 [USA]

The court denied plaintiff AOL's motion for summary judgment seeking to hold defendant liable for violations, inter alia, of the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and common law trespass to chattels, as a result of the transmission of unsolicited bulk e-mail advertising defendant's products to AOL users. The court reached this conclusion because, based on the record before it, it could not determine whether the parties who sent the e-mail in question were defendant's agents, acting under its control, or independent contractors.

C. DEFAMATION

1. Anderson v New York Telephone Co (1974) 35 NY 2d 746) [USA]

The plaintiff was a bishop. A person by the name of Jackson broadcast a program on radio urging the listeners to call up two telephone numbers.

'A person calling these numbers would hear accusations against plaintiff involving him in all sorts of scurrilous activities not the least of which was illegitimately fathering children by women and girls in the church. Jackson's telephones were attached to equipment leased to Jackson by defendant. This equipment contained the recorded messages which would automatically play upon activation of the telephone by a caller.'

The Court held that ... the telephone company's role is merely passive and no different from any company which leases equipment to another for the latter's use ... In order to be deemed to have published a libel a defendant must have had a direct hand in disseminating the material whether authored by another, or not ... It could not be said, for example, that International Business Machines, Inc., even if it had notice, would be liable were one of its leased typewriters used to publish a libel. Neither would it be said that the Xerox Corporation, even if it had notice, could be held responsible were one of its leased photocopy machines used to multiply a libel many times.'

2. Cubby Inc v CompuServe Inc (1991) 776 F Supp 135 [USA]

'Action was brought against computer Service Company for its alleged libel, business disparagement, and unfair competition. On company's motion for summary judgment, the District Court, Leisure, J., held that: (1) computer service company that provided its subscribers with access to electronic library of news publications put

together by independent third party and loaded onto company's computer banks was mere "distributor" of information, which could not be held liable for defamatory statements made in news publications without showing that it knew or had reason to know of defamation'

'CompuServe develops and provides computer-related products and services, including CompuServe Information Service ("CIS"), an on-line general information service or "electronic library" that subscribers may access from a personal computer or terminal. Subscribers to CIS pay a membership fee and online time usage fees, in return for which they have access to the thousands of information sources available on CIS. Subscribers may also obtain access to over 150 special interest "forums," which are comprised of electronic bulletin boards, interactive online conferences, and 349 topical databases.

One forum available is the Journalism Forum, which focuses on the journalism industry. Cameron Communications, Inc. ("CCI"), which is independent of CompuServe, has contracted to "manage, review, create, delete, edit and otherwise control the contents" of the Journalism Forum "in accordance with editorial and technical standards and conventions of style as established by CompuServe".

"New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation. "The requirement that a distributor must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment, made applicable to the states through the Fourteenth Amendment"

CompuServe's CIS product is in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications. CompuServe and companies like it are at the forefront of the information industry revolution. High technology has markedly increased the speed with which information is gathered and processed: it is now possible for an individual with a personal computer, a modem, and telephone line to have instantaneous access to thousands of news publications from across the world.

While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carries the Publication as part of a forum that is managed by a company unrelated to CompuServe.... CompuServe has no more editorial

control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.

"First Amendment guarantees have long been recognized as protecting distributors or publications ...Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes. Such a rule would be an impermissible burden on the First Amendment."... Technology is rapidly transforming the information industry.

A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, a book store, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory Rum Orville statements.'

3. Norway v. Ted Asker and Barium District Court (Norway, 2002) [NORWAY]

The accused was the founder of a far right group in Norway. He was convicted for posting racist material that mixed neo-Nazism, racial hatred, and religion, on a web site. He was held responsible for the material despite the fact that it was posted on a server that was based in the United States.

4. Stratton Oakmont v Prodigy (1995) NY Misc Lexis 229 [USA]

The Court held that 'A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.'

The Court held that computer bulletin boards should generally be regarded in the same context as bookstores, libraries and network affiliates. The Court held that in this case, because of Prodigy's own policies, technology and staffing decisions, the scenario had been altered and the Court held that PRODIGY was a publisher.

5. Zeran v America Online Inc (1997) 129 F 3d 327 [USA]

The Court held that a federal immunity was granted to any cause of action that would make service providers liable for information

originating with a third-party user of the service and that lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions-such as deciding whether to publish, withdraw, postpone or alter content-are barred.

D. COMPUTER FRAUD:

1. FTC v. Craig Lee Hare S.D. Fla. 4/*/98 [USA]

In this case the action was for deceptive trade practices arising from on-line "auction" offering sale of computer products that were never delivered. The Defendant pleaded guilty to wire fraud and was sentenced to six months home detention, three years probation and ordered to pay restitution of over $22,000. He was also barred for life from conducting Internet commerce.

2. United States v. Middleton 35 F. Supp. 2d 1189 (N.D. Cal. 1999) [USA]

The court held that the term "individual" as used in the Computer Fraud and Abuse Act, is not confined to natural persons, but extends to business entities, and hence damage to an ISP-victim was encompassed under the statute.

3. United States v. Hoke Magistrate No. 99-889M (C.D. Cal. 4/14/99) [USA]

A suit was filed against Gary Hoke for disseminating misinformation on a counterfeit Bloomberg News Service Web page regarding an alleged merger between his employer PairGain Technology, Inc. and ECI Telecom, Ltd.

Initial investigation by the FBI revealed that Hoke might have used services of Angelfire.com to host the page and Hotmail email service. Hoke was traced by IP addresses from these services. Hoke, pled guilty and was sentenced to five months of home detention, five years probation, and restitution of $93,086.77.

4. United States v. Pirello 255 F.3d 728 (9th Cir. 2001) [USA]

The Ninth Circuit ruled on the application of the US Sentencing Commission Guidelines (USSG) about a defendant fraudulently selling computers online. The defendant Pirello placed four advertisements on Internet classified-ads websites, soliciting buyers for computers. Pirello received three orders, deposited the money in his personal bank account, and never delivered computers. The court determined that USSG 2F1.1(b)(3), which instructs courts to enhance a sentence by two levels if the offense was committed through "mass-marketing," applied to Pirello's

fraudulent Internet advertisements. The court held that the use of the Internet website to solicit orders for non-existent computers violated the USSG and affirmed the lower court's enhancement of Pirello's sentence.

5. Kennison v Daire (1986) 160 CLR 129 - [AUSTRALIA]

In this case, the accused held an automatic teller machine (ATM) card which enabled him to withdraw funds from his account from a certain bank by inserting the card and keying in his personal identification number; but it was a condition of his use of the card that the customer's account could be drawn against to the extent of the funds available in that account.

The accused closed the account but subsequently used the card to withdraw funds. It was held that it was not sufficient that the bank had programmed the computer to permit the withdrawal, as the bank consented to the withdrawal by the cardholder who presented his personal identification number only if the cardholder had an account, which was current, and accordingly the appellant was guilty of larceny.

The Court further held that "The fact that the Bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the Bank consented to the withdrawal of money by a person who had no account with the Bank. It is not suggested that any person, having the authority of the Bank to consent to the particular transaction, did so. The machine could not give the Bank's consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent".

E. PORNOGRAPHY:

1. Davis v. Gracey 111 F.3d 1472 (10th Cir. 1997) [USA]

After the accused, Davis, sold obscene CD-ROMs to an undercover officer, a warrant was obtained to search his business premises; police officers determined pornographic CD-ROM files could be accessed through the bulletin board and seized the computer equipment used to operate it. Following his criminal conviction and civil forfeiture of the computer equipment in state court proceedings, Davis, his related businesses, and several users of email on his bulletin board brought action against the officers who executed the search, alleging that the seizure of the computer equipment and email and software stored on the system violated constitutional and statutory provisions.

Affirming, the 10th Circuit held that the original warrant was not unconstitutionally overbroad, and that the incidental temporary seizure

of bulletin board email users' files did not invalidate the seizure of the computer within which they were stored. "The computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."

2. United States v. Thomas 74 F.3d 701 (6th Cir. 1996) [USA]

A Bulletin Board Service (BBS) operator in California was arrested and convicted when pornographic materials from their site were downloaded by a federal postal inspector in Tennessee (USA), and materials ordered from them were delivered, violating federal obscenity laws. Conviction and sentence were affirmed.

The Court held that GIF files are not "intangible" for purpose of federal obscenity laws; distribution of obscene materials was "knowing" even without defendants having specific knowledge of each individual transmission; obscenity may be measured by "community standard" in place where materials are received; defendants' ability to control subscriptions and access to their BBS made them liable for the downloading that occurred in Tennessee, and thus amenable to jurisdiction there. The court distinguished the subscriber-BBS from an "Internet-type" situation, in which the person posting the materials has no control over where they will be downloaded.

3. United States v. Kufrovich 997 F. Supp. 246 (D. Conn. 1997) [USA]

Defendant, charged under 18 U.S.C. § 2422(b) and § 2423(b) with using a means of Interstate Commerce to knowingly persuade a minor to engage in sexual activity moved to dismiss, alleging that the Supreme Court's finding that portions of the Communications Decency Act were unconstitutional made Internet speech presumptively protected under the First Amendment. Because Defendant's contact with the victim had been through the Internet, it was constitutionally protected and could not be used in evidence against him, he maintained.

The court rejected the argument, holding that the statutes under which the charges were brought do not impermissibly limit speech; they criminalize the use of means of interstate commerce (such as Internet and telephone lines) for the purpose of luring a minor into sexual activity.

4. M.G. v. Brian D. Travis 667 N.Y.S.2d 11 (1st Dep't 1997) [USA]

The Court upheld the restriction on paroled sex offender's use of computers as within "the spirit and intent of the Legislature in enacting Megan's Law and ... within the responsibility of the Division of Parole".

The Court held that "The imposition of these conditions did not violate the parolee's Double Jeopardy rights and was not arbitrary or capricious". The court held that "this condition is narrowly tailored solely to prevent petitioner from exchanging pornographic messages. Certainly, no lengthy explication is needed, in this age of 'Internet pedophilia,' to show the wisdom of this condition in preventing recidivism".

5. United States v. Hockings 129 F.3d 1069 (9th Cir. 1997) [USA]

It was held that the computer graphic interchange files (GIFs) in binary format fall within the definition of "visual depictions" as contemplated by 18 U.S.C. §§ 2252(a)(1) and (4)(B). The fact that such files require the use of personal computer hardware and software to depict images of child pornography does not put them outside the statute, the court held, analogizing to an earlier case in which undeveloped film was also held to constitute a "visual depiction" under the statute.

6. United States v. Simpson 152 F.3d 1241 (10th Cir. 1998) [USA]

The court held that the Detective's affidavit describing aborted transaction negotiated in Internet chat room to exchange child pornography was sufficient to constitute probable cause in obtaining search warrant.

7. United States v. Matthews 11 F. Supp 2d 656 (D. Md. 1998) [USA]

The Court held that each transfer by email of a child pornography image is a separate offense under federal law. The Court rejected the defendant's argument that the successive email transmissions were all part of a single online "conversation".

The U.S. District Court for the District of Maryland also rejected the defendant's First Amendment defense based on the claim that he was involved in investigative journalism. This decision was affirmed by the Fourth Circuit Court of Appeals.

8. People v. Barrows 677 N.Y.S.2d 672 (Supr. Ct. 1998) [USA]

New York penal code law § 235.22, bars the knowing transmission of sexual materials to a minor by computer with the intent to lure the minor into sexual activity. This deed was held to, prima facie, be unconstitutional. Analogizing to Reno v. ACLU, the Court held that the inherent vagueness of the terms in the code to describe elements of the crime would insidiously end all communication on the Internet related to sex (this would also include communication with regard to say, Sex education). However, § 263.10, prohibiting "promoting an obscene sexual performance by a child" was upheld. The court distinguished the

two code sections, reasoning that the upheld section was unrelated to the age of the recipient of the proscribed communication.

9. Germany v. CompuServe Deutschland, et al (Bavaria 5/28/98) [GERMANY]

German District Court Judge Wilhelm Hubbert convicted Felix Somme, the former head of CompuServe Germany, of child pornography for failing to block third parties' postings of pornographic pictures using CompuServe's services. Somm received two years probation and was fined DM 100, 000, despite the fact that under current German law ISPs are not held responsible for banned information on the Internet if they are unaware of the existence of the material. The conviction was overturned on appeal.

10. United States v. Whiting 165 F.3d 631 (8th Cir. 1999) [USA]

Appeals court held that change of definition of "visual depiction" in law banning child pornography did not violate ex post facto clause because previous definition already included data stored on computer disks, although not explicitly. Amendment made to include electronic data was a clarification rather than a substantive change.

11. Fedeemer v. Haun 35 F. Supp. 852 (D. Utah 1999) [USA]

Plaintiff challenged Utah's sex offender notification statute, which would make sex offender registry information available to the general public without restriction on the Internet. The court held that the registry information posted on the Web site and available to a global audience that will have no risk of encountering the offender was not reasonably related to the non-punitive goal of preventing additional sex offences and therefore violated the Double Jeopardy and Ex Post Facto Clauses.

The court held that the statute did not violate the Equal Protection Clause because it was rationally related to the goal of guarding against sexual offenses. The Court also held that the Due Process Clause was not violated because the information to be posted is considered "non private" and therefore there is no cognizable injury to the plaintiff's reputation. The defendant, the Utah Department of Corrections, stipulated it would administer the statute in accordance with the court's decision, and therefore no order was issued.

12. Free Speech Coalition v. Reno 198 F.3d 1083 (9th Cir. 1999) [USA]

Action challenging constitutionality of certain provisions of the Child Pornography Prevention Act of 1996 (CPPA), which make it

illegal to post on the Internet or to show in movies, pornographic images of adults portrayed as minors.

Court held that CPPA was unconstitutional insofar that it describes as child pornography, computer images that do not involve the use of real children in their production or dissemination. Language used in the statute, prohibiting images that "appear to be a minor" and "convey the impression" of being a minor, was held to be unconstitutionally vague.

The court also noted that Congress has not articulated a compelling interest sufficient to withstand strict scrutiny. These specific provisions were struck down, but the remainder of CPPA was allowed to stand. Later, the US Supreme Court, quashing the decision, granted Certiorari.

13. People v. Foley No. 17 (N.Y. Ct. App., Apr. 11, 2000) [USA]

The court found that the state law against knowingly transmitting sexually explicit communications to minors with intent to lure them into sexual activity was constitutional and did not violate the Commerce Clause. The court noted that the statute is no broader than necessary to achieve the purpose of preventing the sexual abuse of children.

14. State of New York v. BuffNet NY Appellate Division, Fourth Judicial Department (2001) [USA]

An Internet Service Provider (ISP) pled guilty to the misdemeanor charge of knowingly providing access to child pornography. A two-year investigation found that ISP, BuffNet, knowingly hosted a child pornography newsgroup called "Pedo University". The police notified BuffNet that they were hosting illegal content, yet BuffNet failed to remove the newsgroup from its servers. Police then seized the ISP's servers. BuffNet was levied a $5000 fine, and removed the obscene content.

15. John Robin Sharpe v. B.C 2001 SCC 2. File No.: 27376. (Canada, 2001) [CANADA]

The Supreme Court of Canada upheld a law that makes it a crime to possess child pornography. In 1999 a trial court had struck down the law and dismissed charges against John Robin Sharpe who had been charged under the law. In a 9-0 decision the court upheld the law, but created two exceptions. One was to protect private works of the imagination or photographic depictions of oneself, and another for those that create sexually explicit depictions of children for their own personal pleasure.

16. Regina v. Vernon Boyd Logan No. 9317 Port Hardy Registry [CANADA]

The accused had pleaded guilty to possession of child pornography, contrary to section 163.1(4) of the Criminal Code. The police had seized a variety of child pornography, mostly magazines containing photographs of physically mature teenaged boys performing sexual acts with each other, from the home of the accused. Some pictures were of pubescent boys and girls involved in sexual activities together, and a few depicted pubescent girls engaging in similar behavior.

It was not alleged that the accused had created, published, imported, distributed, or sold child pornography, or had it in his possession for any of those purposes. Moreover, there was no suggestion that the defendant has been sexually involved with children, or that the pornography had been inspired any deviant behavior by him. The accused was given an absolute discharge. The Court held that the act of merely possessing child pornography was "entirely passive". The Court held that the accused did not pose any threat to the public, as the extent of his culpability was that he had prohibited material in his possession and, presumably, read it.

F. ONLINE GAMBLING

1. Olivier v. Ministry of Safety and Security, Province of Gauteng High Court of South Africa, Witwatersrand Div., 10/97 [SOUTH AFRICA]

On application of owner for return of certain computer equipment seized in a search, a South African court held the impoundment lawful on the grounds that it was used for online gambling in contravention of South African law.

2. State of New York v. World Interactive Gaming Corp 1999 N.Y. Misc. LEXIS 425 (N.Y. App. Div. 1999) [USA]

Court granted injunction barring Antigua-based online gaming company from doing business with New York residents. The court held that regardless of whether gambling is legal where the company is based, the act of entering the bet and Transmitting the information from New York via the Internet is adequate to constitute gambling activity within New York State. The company required users to enter a physical address, and rejected customers whose address was in a state where gambling was illegal. However, the New York attorney general used Nevada address from New York and was able to gain access. The court held this attempt to screen users was not sufficient to shield the site from liability.

3. Reference Re Earth Future Lottery (P.E.I.), 2002 PESCAD 8 (Canada 2002) [CANADA]

The Prince Edward Island Supreme Court ruled that a charitable lottery was illegal under the Canadian criminal code.

Earth Future Lottery had been granted a license to operate an Internet lottery from its headquarters on Prince Edward Island. The Canadian Criminal Code generally prohibits lotteries, but allows charitable lotteries conducted within their own provinces. The court ruled that although the Internet lottery would operate from Prince Edward Island, it would also reach other provinces and thus it violated the Canadian Criminal Code.

4. United States v. Cohen 260 F.3d 68 (2d Cir. 2001) [USA]

The Court of Appeals affirmed a decision by a lower court convicting Jay Cohen of operating an illegal offshore Internet sports gambling operation. Cohen operated a bookmaking organization located in Antigua. Customers were required to maintain accounts with the business, and would contact the organization by telephone or Internet to request particular bets. The organization would issue an acceptance and confirmation of each bet.

The Court of Appeals held that the safe harbor provision of 18 U.S.C.S. § 1084(b), which shield an individual from criminal liability under certain circumstances, did not apply. The court noted that betting is illegal in New York, and that Cohen's customers were placing bets by requesting the bets and having them accepted. In addition, the court found that Cohen had the requisite means rea, as it was not necessary that he intended to violate the statute so long as he knowingly committed the criminal acts.

G. MISCELLANEOUS

1. Register.com, Inc. v. Verio, Inc 126 F. Supp. 2d 238 (S.D.N.Y., December 12, 2000) [USA]

Court issued a preliminary injunction enjoining Verio, Inc. from either utilizing a search robot to obtain information from Register.com's Whois database, or utilizing information derived from that database for mass unsolicited advertising by telephone, direct mail or electronic mail.

Court held that Verio's actions would likely constitute a breach of plaintiff's Terms of Use, as well as a violation of both the Computer Fraud and Abuse Act and the Lanham Act and a trespass to chattels. In reaching this conclusion, the court held that Register.com's Terms of Use are likely to create a contract between

Register.com and the users of its Whois database, notwithstanding the fact that these users are not required clicking an "I Agree" button indicating their agreement to be so bound.

2. United States v. Gilboe 684 F.2d 235 (2d Cir. 1982) [USA]

The Court convicted a person for transportation of money obtained by fraud. Defense based on contention that electronic transfer was not "transportation" was rejected.

3. People v. Alan Munn Crim. Court Queens City., No. 98Q-052574 [USA]

The defendant in a harassment case, who asked the readers of a posting on an Internet news group to kill a police officer with family, moved to dismiss on the grounds that New York statute did not cover the Internet. Statute covered communications "by telephone, or telegraph, mail or any other form or written communication". The Judge held that posting was covered because it was initiated by means of a telephonic communication with the network community.

4. State of Utah v. Amoroso 364 Utah Adv. Rep. 3 (Utah Ct. App. 1999) [USA]

The state of Utah may criminally prosecute an Illinois corporation for liquor sales to Utah residents over the Internet, through the use of a telephone "800" number, and by mail. Although the Utah appellate court held that it was improper to apply the civil "minimum contacts" analysis, the court held that there was criminal personal jurisdiction in Utah over the defendants based upon the theory that the conduct committed in Illinois caused an unlawful result in Utah. The court also held that the prosecution was valid under the Twenty-First Amendment and did not violate the Commerce Clause.

5. United States v. Baker (890 F. Supp. 1375 (E.D. Mich. 1995) [USA]) aff'd sub nom U.S. v. Alkahabaz (104 F.3d 1492 (6th Cir. Mich. 1997) [USA])

In this case, a college student who wrote a sado-masochistic fantasy story about one of his classmates and transmitted it to an Internet correspondent could not be prosecuted for interstate transmission of threats to injure or kidnap as there was no showing that the thoughts expressed in the story were "true threats" on which the student intended to act.

On January 29, 1997, on appeal in U.S. v. Alkhabaz, dismissal was affirmed. The Court held that the elements of the charge of threat were not met by email transmitted between two Internet users containing sado-masochistic fantasies about a student known to one of the correspondents.

6. State of Pennsylvania v. Murgalis No. 189 MDA 1999 (Pa. Super. Ct., June 2, 2000) [USA]

The Pennsylvania Superior Court held that the Internet falls under the definition of a "computer system" and the use of e-mail is "accessing a computer" under a Pennsylvania criminal statute. The defendant was convicted of unlawful use of a computer, arising from his failure to deliver items purchased on-line by customers, and his passing of bad cheques to suppliers. The Pennsylvania statute prohibits the use of a computer system with the intent to defraud. The court rejected the defendant's argument that the Internet is not a "computer system".

7. United States v. Sills S.D.N.Y., April 2000 [USA]

A police officer was charged with using software and a radio scanner to intercept alphanumeric pager messages in violation of the Electronic Communications Privacy Act. The judge denied the officer's motion to dismiss, holding that the interception did not fall within the Act's exemption for tone-only pagers, and rejecting a claim of selective prosecution.

8. Firth v. State of New York N.Y. Court of Claims, March 2000 [USA]

The plaintiff claimed that publication of an alleged libel on the Internet was "continuous publication", which would extend the statute of limitations. The court held that the statute would run from the date the material was first posted, rather than continuously. On October 29, 2001, the New York Appellate Division Court affirmed the decision.

9. United States v. Gray 78 F. Supp.2d 524 (E.D. Va. 1999) [USA]

The court held that child pornography discovered during a search conducted pursuant to obtaining a warrant for materials related to computer tampering was admissible. Defendant argued that files with the .JPG extension were presumptively pictures and not related to subject of search. Court noted that hackers frequently mislabel files, and FBI agents were not required to take file names at face value.

10. Doherty v. Registry of Motor Vehicles 97CV0050 (Mass. Dist. Ct., Suffolk Cty. Charlestown Div., May 28, 1997) [USA]

The court held that an electronically-transmitted police report satisfied the requirement of a signed writing under the state's perjury law.

11. In re Double-click Inc. Privacy Litigation 00 Civ. 0641 (S.D.N.Y., March 28, 2001) [USA]

The Court dismissed the claims advanced by the plaintiff under the Electronic Communications Privacy Act, the Computer Fraud and

Abuse Act, and the Wiretap Act arising out of Doubleclick's use and placement of "cookies" on plaintiffs' computers. Doubleclick uses such "cookies" to gather information about the users' use of Doubleclick client web sites. Since Doubleclick's clients consented to such information being gathered, the court held that Doubleclick's activities did not run afoul of either the Electronic Communications Privacy Act or the Wiretap Act. The court also dismissed the claims, which the plaintiffs advanced under the Computer Fraud and Abuse Act because any damages caused by Doubleclick's activities did not meet the threshold required by the Computer Fraud and Abuse Act. Finally, the court, having dismissed all of the plaintiffs' federal claims, declined to retain jurisdiction over plaintiffs' state law claims, and dismissed the action.

12. United States Of America V. Robert Tappan Morris 928 F.2d 504; 1991 U.S. App. LEXIS 3682 United States Court Of Appeals For The Second Circuit[USA]

In 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

known as the Internet "worm" or "virus". The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was the release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into the Internet.

Morris sought to program the INTERNET worm to spread widely without drawing attention to it. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.

Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. Multiple copies of the worm on a computer would make the worm easier to detect and would bog down

the system and ultimately cause the computer to crash. Therefore, Morris designed the worm to "ask" each computer whether it already had a copy of the worm. If it responded "no," then the worm would copy onto the computer; if it responded "yes," the worm would not duplicate. However, Morris was concerned that other programmers could kill the worm by programming their own computers to falsely respond "yes" to the question. To circumvent this protection, Morris programmed the worm to duplicate itself every seventh time it received a "yes" response.

As it turned out, Morris underestimated the number of times a computer would be asked the question, and his one-out-of-seven ratio resulted in far more copying than he had anticipated. The worm was also designed so that it would be killed when a computer was shut down, an event that typically occurs once every week or two. This would have prevented the worm from accumulating on one computer, had Morris correctly estimated the likely rate of re-infection. Morris identified four ways in which the worm could break into computers on the network: through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer; through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer; through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and re-infecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around USA either crashed or became "catatonic". When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent re-infection. However, because the network route was clogged, this message did not get through until it was too late.

Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $ 200 to more than $ 53,000.

Morris was found guilty, following a jury trial, of violating 18 U.S.C. @ 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $ 10,050, and the costs of his supervision.

The major issue raised in this case was what satisfies the statutory requirement of "access without authorization". Subsection 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization". The accused contended that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes.

The Court held that under the traditional standard Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

The Court held that Morris's conduct fell well within the area of unauthorized access. "Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers".

The Court also held that although initial insertion of the worm simply exceeded the accuser's authorized access, the evidence demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program.

Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. The Court held that the evidence supported the conclusion that the accused accessed without authority as opposed to merely exceeding the scope of his authority.

Chapter–17
E-mail related Crime

1. **What is E-mail**
2. **What is Tracing of E-mail source**
   - a. **Spoofing**
   - b. **Remaining**
   - c. **Relaying**
   - d. **Spamming**
   - e. **Stealing**
   - f. **Bogus accounts**
3. **Life Cycle of E-mail**
4. **Email related Crime**
   - a. **Email spoofing**
   - b. **Sending malicious codes through email**
   - c. **Email bombing**
     - a. **Sending threatening emails**
     - b. **Defamatory emails**
     - c. **Email frauds**
5. **Denial of Service tools (DoS)**

---

1. What is E-mail:

E-mail is meant for electronic mail. Another common spelling for e-mail is email.

It is the transmission of messages over computer communications networks. Almost mainframes, minicomputers, and computer networks have an e-mail system. Some electronic-mail systems are confined to a single computer system or network. But others have gateways to other computer systems, enabling users to send electronic mail anywhere in the world. Companies that are fully computerized make extensive use of e-mail because it is fast, flexible, and reliable.

Computer e-mail systems include an initial text editor for composing messages. Any one can send message to the recipient by specifying the recipient's address. The same message can be sand to several users at once. This is called broadcasting.

Sent messages are stored in electronic mailboxes. The recipient fetches them. So it is the duty of the recipient to check his electronic mailbox periodically. After reading the mail, it can store it in a text file, forward it to other users, or delete it. Copies of memos can be printed out on a printer.

All online services and Internet Service Providers (ISPs) offer e-mail and most also support gateways so that any body can exchange mail with users of other systems. Usually, it takes only a few seconds or minutes for mail to arrive at its destination. This is a most effective way to communicate with a group by broadcasting a message or document to everyone in the group at once.

Different e-mail systems use different formats. These are as follows:

1. In the PC world, an important e-mail standard is MAPI.
2. The CCITT standards organization has developed the X.400 standard, which attempts to provide a universal way of addressing messages.
3. To date the de facto addressing standard is the one used by the Internet system because almost all e-mail systems have an Internet gateway.

2. What is Tracing of E-mail source

E-mail is the most common security vulnerability. It is a virtual door that leads directly into the network. It can be used by hackers to sneak into, or by staff to sneak secrets out. It can also be used as a portal for data destruction. It is important to know how to handle e-mail incursions.

E-mail Tracing is the most common duty of cyber crime investigators. An audit or paper trail of e-mail traffic is the most common type of evidence used in court. Forensic tracing of e-mail is similar to traditional gumshoe detective work. Checking involves looking at each point through which an e-mail passed, with the detective working step-by-step back to the originating computer, and, eventually, the perpetrator. The process requires knowing how e-mail works.

All e-mail contains HEADERS. Tracing of external e-mail can be done by looking at the message-header information. The message header provides an audit trail of every machine an e-mail has passed through. Some places the e-mail has traveled will be unfamiliar machine names outside the company network. A more sophisticated online free tracing tool like Web tracer may be needed.

Ways of FAKING E-MAIL These are -

a. Spoofing
b. Remailing
c. Relaying
d. Spamming
e. Stealing
f. Bogus accounts

a. SPOOFING: Spoofing is an e-mail made to appear to recipient computer which come from someone E-mail other than the real sender. The e-mailer uses a software tool that is readily available off the Internet to cut out his IP address and replace it with someone else's address. The first machine to receive the spoofed message records the real IP address of the machine sending the message even though the faked ID is in the header.

b. REMAILING: Remailing is an attempt made to throw tracing or tracking off the trail by sending the e-mail to a computer that strips the sender's IP address and remails it with the remailing computer's IP address. The only way to find out who sent the mail is to look at any logs maintained by these remailer or anonymizer companies. Their stated policies, however, include the proviso that they don't keep logs. About the only thing an investigator can do is closely analyzing the message for embedded information that might give clues to the user or system that sent the message.

c. RELAYING: Relaying is when someone hides the origin of an e-mail message to have someone else's mail server send the message. A properly configured mail server will only process mail from within its system and won't relay mail from IP addresses originating from outside its network. But if the mail server is not configured properly, it becomes vulnerable to a wide variety of remote access programs.

d. SPAMMING : Spamming occurs when an e-mail message is sent with a large number of recipients, usually routed through an unsuspecting company's mail server. The e-mailer uses it as a relay point, and the owner of the server may never be aware that the e-mailer has been there. The e-mailer then disappears before anyone gets suspicious. This is not only a theft of services, but potentially a denial of services as well, if the volume of e-mail sent through the server causes it to crash.

e. STEALING: Stealing can be broadly defined as unauthorized use of someone else's password and e-mail account. Some common ways in which stealing occurs are shoulder-surfing or sniffing a network (watching all the network traffic and intercepting user IDs and passwords).

f. BOGUS ACCOUNTS: Bogus Accounts free mails are quite common. Anybody can give a false identity and address when opening up a Hotmail account It is difficult to catch someone who has done this because the e-mail company never knows who opened the false account, and like disposable cell phones. These accounts are quickly used and discarded. Pornographers often use this trick.

looking at when they read their mail. In the common case of an Internet Service Provider whose users dial in from their home computers, the client computer is the user's home machine, and the "server" is some machine that belongs to the ISP.

To send email, the user usually composes the message on his own computer and then sends it off to the ISP's mail server. At this point the computer is finished with the job, but the mail server still has to deliver the message. It does this by finding the recipient's mail server, talking to that server and delivering the message. It then sits on that second mail server until. When the recipient comes to read the mail, then he retrieves it onto his own computer normally deleting it from the mail server in the process. A typical email passes through many computers during its lifetime.

4. Email related Crime:

Email has fast emerged as the world's most preferred form of communication. Billions of email messages traverse the globe daily. Like any other form of communication, email is also misused by criminal elements. The ease, speed and relative anonymity of email has made it a powerful tool for criminals. Some of the major email related crimes are:

a. Email spoofing
b. Sending malicious codes through email
c. Email bombing
d. Threatening emails
e. Defamatory emails
f. Email frauds

a. Email spoofing: A spoofed email is one that appears to originate from one source but has actually emerged from another source. Email spoofing is usually done by falsifying the name and / or email address of the originator of the email. Usually to send an email the sender has to enter the following information:

i. Email address of the receiver of the email
ii. Email address of the person who will receive a copy of the email (referred to as CC for carbon copy)
iii. Email address of the person who will receive a copy of the email (referred to as CC for carbon copy & BCC for blind carbon copy)
iv. Subject of the message (a short title / description of the message)

b. Sending malicious codes through email

1. Trojans,
2. viruses,
3. worms.

Emails are often the fastest and easiest ways to propagate malicious code over the Internet. The Love Bug virus, for instance, reached millions of computers within 36 hours of its release from the Philippines thanks to email.

Hackers often bind Trojans, viruses, worms and other computer contaminants with e-greeting cards and then email them to unsuspecting persons. Such contaminants can also be bound with software that appears to be an anti-virus patch. The email informs him that the attachment contained with the email is a security patch that must be downloaded to detect a certain new virus.

c. Email bombing: Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account or servers crashing.

A simple way of achieving this would be to subscribe the victim's email address to a large number of mailing lists. Mailing lists are special interest groups that share and exchange information on a common topic of interest with one another via email. Mailing lists are very popular and can generate a lot of daily email traffic - depending upon the mailing list. Some generate only a few messages per day others generate hundreds. If a person has been unknowingly subscribed to hundreds of mailing lists, his incoming email traffic will be too large and his service provider will probably delete his account. The simplest email bomb is an ordinary email account.

There are several hacking tools available to automate the process of email bombing. These tools send multiple emails from many different email servers, which make it very difficult, for the victim to protect himself.

d. Threatening emails: Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.

e. Defamatory emails : Defamatory emails have been discussed earlier cyber-defamation or even cyber-slander as it is called can prove to be very harmful and even fatal to the people who have been made its victims.

f. Email Frauds: Email spoofing is very often used to commit financial crimes. It becomes a simple thing not just to assume someone else's

identity but also to hide one's own. The person committing the crime understands that there is very little chance of his actually being identified.

5. Denial of Service (DoS) Attack:

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. Usually these attacks do not necessitate the need to get access into anyone's system.

These attacks have been getting decidedly more popular as more and more people realize the amount and magnitude of loss, which can be caused through them. The other good reason also may be that a business may want to harm a competitor by crashing its systems.

The victim of such an attack may see many such demands coming from computers from around the world. Unfortunately, to be able to gain control over a malicious denial-of-service attack would require tracing all the computers involved in the attack and then informing the owners of those systems about the attack. The compromised system would need to be shut down or then cleaned. This process, which sounds fairly simple, may prove very difficult to achieve across national and later, organizational borders.

Even when the source(s) of the attack are traced there are many problems, which the victim may be faced with. He will need to inform all the involved organizations in control of the attacking computers and ask them to either clean the systems or shut them down. Across international boundaries this may prove to be a titanic task. The staff of the organization may not understand the language. They may not be present if the attack were to be launched during the night or during weekends.

The computers that may have to be shut down may be vital for their processes and the staff may not have the authority to shut them down. The staff may not understand the attack, system administration, network topology, or any number of things that may delay or halt shutting down the attacking computer(s). Or, more simply, the organization may not have the desire to help.

If there are hundreds or even thousands of computers on the attack, with problems like the ones mentioned above, the victim may not be able to stop the attack for days by which time the damage would have been done. His servers would be completely incapacitated to administer to so many demands and consequently would crash.

It is very simple for anyone to launch an attack because denial-of-service tools can easily be procured from the Net. The major versions of distributed denial of service attack tools are Trinoo, TFN, TFN2K and Stacheldraht. Denial-of-Service tools allow the attackers to automate and preset the times and frequencies of such attacks so that the attack is launched and then stopped to be launched once again later. This makes it very difficult, in fact almost impossible, to trace the source of the attack.

These tools also provide another service by which the attacking computer can change its source address randomly thereby making it seem as if the attack is originating from many thousands of computers while in reality there may be only a few.

Distributed denial-of-service attacks are a very perturbing problem for law enforcement agencies mainly because they are very difficult to trace. In addition, usually these attacks are directed towards very sensitive systems or networks sometimes even those that are vital to national security. Sometimes, even when the perpetrators can be traced, international extradition laws may prove to be a hitch in bringing them under the authority of the law.

The other types of DoS attacks are Ping of Death and SYN attacks. A Ping of Death attack involves a very large Internet Control Messaging Protocol (ICMP) packet and the receiving computer gets it in the form of data packets. Then it tries to reassemble it. When reassembled the packet proves to be too large for the buffers making the buffers overflow.

The SYN attack involves the three-way handshake of the TCP/IP protocol. First the client sends a SYN packet to the server. Then the server responds with a SYN-ACK. When the client responds to this, only then does the client-server connection really start. Now in a SYN attack the client does not respond to the SYN-ACK. It waits till just before the service time expires and then sends another request. This way the server machine remains engaged. The above given process keeps on getting repeated till the server machine crashes.

Denial of Service is a generic term for a type of attack. This can take many forms. The Melissa virus came to be called a denial of service attack. Because it clogged networks and servers with the e-mail it generated.

Chapter–18
Digital Signature, Electronic Signature, Cryptographic Signature

A. What is Digital Signature :

In cryptography, a digital signature or digital signature scheme is used to pretend the security properties of a signature in digital form. Digital signature schemes normally give two algorithms-

1. One for signing which involves the user's secret or private key,
2. Other for verifying signatures which involves the user's public key.

The output of the signature process is called the digital signature. Digital signatures are like as written signatures. They used to provide authentication of the associated input, usually called a message. Messages may be anything, from electronic mail to a contract, or even a message sent in a more complicated cryptographic protocol.

Digital signatures are used to create Public Key Infrastructure (PKI) schemes. User's public key is tied to a user by a digital identity certificate issued by a certificate authority. PKI schemes attempt to unbreakably bind user information such as name, address, phone number, etc. to a public key. So the public keys can be used as a form of identification.

Digital signatures are often used to implement electronic signatures. In a broader term it refers to any electronic data that carries the intent of a signature. But all electronic signatures are not use as digital signatures. In some countries like the United States of America, and in the European Union, electronic signatures have legal significance. But laws concerning electronic signatures do not always make clear their applicability towards cryptographic digital signatures, leaving their legal importance some what unspecified.

1. History:

Martin Hellman first described the notion of a digital signature scheme. Afterwards, Ronald Rivest, Adi Shamir, and Len Adleman invented the RSA algorithm, the first scheme for digital signatures The first widely marketed software package was Lotus Note 1.0. It was released in 1989. It used the RSA algorithm to offer digital signature. RSA signatures are performed using the algorithms of the RSA cryptosystem. Other digital signature schemes were soon developed.

After RSA, the earliest other digital signatures were Lamport signatures, Merkle signatures, known as Merkle trees or simply Hash trees, and Rabin signatures. In 1988, Shafi Goldwasser, Silvio Micali, and Ronald Rivest became the first to rigorously define the security requirements of digital signature schemes.

2. Trapdoor permutation:

A trapdoor permutation was most early signature schemes. A trapdoor permutation family is a family of permutations, specified by a parameter. It is easy to compute in the forward direction, but is difficult to compute in the reverse direction. For every parameter there is a trapdoor that enables easy computation of the reverse direction.

Trapdoor permutations can be viewed as public-key encryption systems. The parameter is the public key and the trapdoor is the secret key. Where encrypting corresponds to computing the forward direction of the permutation and decrypting corresponds to the reverse direction.

Trapdoor permutations can also be viewed as digital signature schemes. Here computing the reverse direction with the secret key is thought of as Signing Key and computing the forward direction is to verify signatures. Digital signatures are often described as public-key cryptosystems, Signing is equivalent to decryption and Verification is equivalent to encryption.

3. Benefits of Digital Signature

a. Authentication

b. Integrity

a. Authentication

Messages may often include information about the entity sending a message. That information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

b. Integrity:

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message. It may be possible to change an encrypted message without understanding it. However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

4. Drawbacks of Digital Signature:

a. Non-Repudiation

b. Association of Digital Signatures and trusted time stamping:

Digital signatures have usefulness. But it does not alone solve all the problem. There are some drawbacks stated below:

a. Non-Repudiation:

In a cryptographic context, the word repudiation refers to the act of disclaiming responsibility for a message. A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult. The recipient can show the signed message to a third party (eg, a court) to reinforce a claim as to its signatories and integrity. The loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly from that user,

are suspect. A user cannot repudiate a signed message without repudiating their signature key.

b. Association of Digital Signatures and trusted time stamping:

Digital signature algorithms and protocols do not inherently provide certainty about the date and time at which the underlying document was signed. The signer might, or might not, have included a time stamp with the signature. In the first case the document itself might have a date mentioned on it. But in later case reader cannot be certain the signer. For instance, backdate the date or time of the signature. Such misuse can be made impracticable by using trusted time stamping in addition to digital signatures.

c. Using Digital Signatures with Trusted applications:

One of the main differences between a digital signature and a written signature is that the user does not see what he signs in digital signature. It is the application that presents a hash code to be encrypted with the private key. But in the case of a malicious application a hash code of another document might be presented. So that the users thinks he is signing the document he sees on the screen but is unwillingly signing another.

5. Legal and Practical aspacts:

Digital signature schemes all have several prior requirements without which no such signature can mean anything, whatever the cryptographic theory or legal provision.

1. Quality Algorithms : Some public-key algorithms are known to be insecure, practicable attacks against them having been discovered.

2. Quality implementation: An implementation of a good algorithm (protocol) with mistake will not work.

3. Distribution of public keys must be done in such a way that the public key claimed to belong to, say, Bob actually belongs to Bob, and vice versa. This is commonly done using a public key infrastructure and the public key user association is attested by the operator of the PKI (called a certificate authority). For open PKIs in which anyone can request such an attestation, the possibility of mistaken attestation is non trivial. Commercial PKI operators have suffered several publicly known problems. Such mistakes could lead to falsely signed, and thus wrongly attributed, documents. closed PKI systems are more expensive, but less easily subverted in this way.

4. Users and their software must carry out the signature protocol properly. Only if all of these conditions are met will a digital signature actually be any evidence of who sent the message, and therefore of their assent to its contents. Legal enactment cannot change this reality of the existing engineering possibilities, though some such have not reflected this actuality.

Legislatures, being importuned by businesses expecting to profit from operating a PKI, or by the technological avant-garde advocating new solutions to old problems, have enacted statutes and / or regulations in many jurisdictions authorizing, endorsing, encouraging, or permitting digital signatures and providing for their legal effect.

The first appears to have been in Utah in the United States, followed closely by the states Massachusetts and California. Other countries have also passed statutes or issued regulations in this area as well and the UN has had an active model law project for some time. These enactments vary from place to place, have typically embodied expectations at variance with the state of the underlying cryptographic engineering, and have had the net effect of confusing potential users and specifiers.

Adoption of technical standards for digital signatures have lagged behind much of the legislation, delaying a more or less unified engineering position on interoperability, algorithm choice, key lengths, and so on what the engineering is attempting to provide.

In several countries, a digital signature has a status somewhat like that of a traditional pen and paper signature. Generally, these provisions mean that what is digitally signed legally binds the signer of the document to the terms therein. For that reason, it is often thought best to use separate key pairs for encrypting and signing. Using the encryption key pair a person can engage in an encrypted conversation, but does not legally sign every message he sends. Only when both parties come to an agreement do they sign a contract with their signing keys, and only then are they legally bound by the terms of a specific document. After signing, the document can be sent over the encripted link.

B. ELECTRONIC SIGNATURE

1. What is Electronic Signature?
2. History and examples of use:
3. Legality of Electronic Signature

4. Laws regarding use of electronic signature
5. Electronic Signature Vendors
6. Pseudo-legal use of imputed electronic signatures

1. What is Electronic Signature:

The term electronic signature has several meanings. USA and other common law contains references to telegraph signatures and faxed signatures, some as far back as the mid-19th century. US Federal Rules of Evidence 1001, 1002, and 1003, among others, give good support for the proposition that electronic records and signatures would be admissible in court. The definition of Electronic Signature comes from the Uniform Electronic Transactions Act (UETA) released by NCCUSL in 1999. It defines that,

"Electronic Signature means an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

The U.S.A. E-Sign Act of 2000 enacted on a federal level many of the core concepts of UETA.

There is confusion between the terms electronic signature and digital signature. An information theory or cryptography background, use digital signature. A digital signature protocol using cryptographic techniques, is sometimes applied to an electronic document. The terms interchangeably, leading to considerable confusion. A cryptographic signature techniques are very different, than other electronic signatures and have extremely different security properties. Digital signature is properly a subset of electronic signature.

2. History of Electronic Signature use:

Before the USA Civil War 1860, Morse Code was used to electronically send messages via telegraph. An early acceptance of the enforceable validity of electronic signatures of this kind came from the New Hampshire Supreme Court in 1869. But it was the invention of electronic communication methods which brought electronic signature into everyday use.

In the 1980's, many companies and even some progressive individuals began using fax machines for high priority or time sensitive delivery of paper based documents. Although a signature in such cases was typically on a piece of physical paper, the image capturing process and the transmission of a copy of the signature was done electronically.

Courts in various jurisdictions have decided that enforceable electronic signatures can include agreements made via email, by entering a Person Identification Number (PIN) into an ATM bank machine, 'signing' a credit/debit slip with a digital pen pad device at a sales counter, acceptance of the terms of an End-User License Agreement via clickwrap when installing software or by signing electronic documents online.

3. Legality of Electronic Signature

Ligality of electronic signature classified as

a. Legal Definitions

b. Legal Test of electronic signature

a. Legal Definitions:

Various laws have been passed internationally to facilitate commerce by the use of electronic records and signatures in interstate and foreign commerce. The intent is to ensure the validity and legal effect of contracts entered into electronically, for instance, ESIGN Act Sec 106 definitions. Some Definitions are given below

ELECTRONIC: The term `electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

ELECTRONIC RECORD: A. The term `electronic record' means a contract or other record created, generated, sent, communicated received, or stored by electronic means

B. Means a record created, generated, sent, communicated, received, or stored by electronic means

ELECTRONIC SIGNATURE

1. The term **`electronic signature'** means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. [GPEA Sec 1710 definitions]

2. The term **"electronic signature"** means a method of signing an electronic message that –

(I) identifies and authenticates a particular person as the source of the electronic message; and

(II) indicates such person's approval of the information contained in the electronic message. UETA Sec 2 definition

3. **Electronic Signatire** means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Federal Reserve 12 CFR 202 definitions refers to the ESIGN Act. [Commodity Futures Trading Commission 17 CFR Part 1 Sec. 1.3 definitions]

4. **Electronic signature** means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the recor [Food and Drug Administration 21 CFR Sec. 11.3 definition]

5. **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

6. **Digital signature:** Digital Signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

7. **Electronic agent : Electronic Agent** means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual

b. Legal Test of electronic signature:

In law, if a signature on a contract or other document is contested, the signature must meet certain tests before a court will uphold them if contested. These requirements vary by jurisdiction, but various sorts of signatures, some entirely electronic Telex addresses (for example, ABC Company sends a Telex to XYZ Company making an offer at a particular price. The offer was held to be binding when the 'signature' was challenged.), telegrams (for example, "I ACCEPT, SMITH" even though Smith never actually touched the telegraph key), and faxes of documents, even in some cases where the original was not signed by the sender.

A central question in such cases is forgery and spoofing of assent, and in these decisions, courts have held that forgery and spoofing can be in practice ruled out. Nevertheless, it is easily possible, for many electronic methods of signature, or imputed signature, to forge or spoof assent. The rapidly rising problem of identity theft illustrates the case of such forgeries.

Often, businesses rely on other means to attempt to ensure an electronic signature is correct, including talking with the signing person directly or over the phone before an electronic signing, having an ongoing business relationship, and receiving payment or other indications of intent to do business that do not rely solely on a signed document. This is good business practice even in the paper world, as forgeries have been common there since time immemorial. Fraud is a common issue in all signature situations, and neither type of signature (paper or electronic) provides fully effective anti-fraud protections.

None of the electronic signatures in these examples are digital signatures in that there is no cryptographic assurance of the sender's identity, and no integrity check on the text received. However, all are electronic signatures, and all have been found legaly binding in some circumstances.

4. Laws regarding use of Electronic Signature

The following are the International laws used for E-signature

1. Croatia - Zakon o elektronickom potpisu - nn 10/02
2. U.S. - Electronic Signatures in Global and National Commerce Act
3. U.S. - Uniform Electronic Transactions Act - adopted by 48 states
4. U.S. - Digital Signature And Electronic Authentication Law
5. U.S. - Government Paperwork Elimination Act (GPEA)
6. U.S. - The Uniform Commercial Code (UCC)
7. UK - s.7 Electronic Communications Act 2000
8. European Union - Electronic Signature Directive (1999/93/EC)
9. Türkiye - Electronic Signature Law
10. China - Law of the People's Republic of China on Electronic
11. Signature (effective April 1, 2005)
12. Mexico - E-Commerce Act [2000]
13. Costa Rica - Digital Signature Law 8454 (2005)
14. Slovenia Slovene Electronic Commerce and Electronic Signature Act
15. South Africa - The Electronic Communications and Transactions Act 25, 2002

5. Electronic Signature Vendors

The followings are the Electronic Signature Vendors, working internationally.

1. ARX,
2. DocuSign,
3. EchoSign iDentifi.eSign,
4. Orion Systems,
5. Sertifi,
6. Silanis,
7. Softpro: SignDoc,
8. Topaz Systems,
9. Yozons

6. Pseudo-legal use of imputed electronic signatures

Some web sites and software EULAs contain terms that assert that various electronic and other actions give rise to legally effective signatures. For example, a web page might announce that, by accessing the site at all, you have agreed to a certain set of terms and conditions. A software product might assert, in its packaging or on an early installation screen, that by using it any body have agreed to licensing terms. These may or may not have been discernible prior to sale. This may or may not be completely displayed even at installation.

These licenses often include such restrictions as a prohibition of reviewing the product for publication without prior permission of the publisher / distributor, or prohibition on studying the product for an otherwise lawful purpose such as producing data files in a compatible format. Some such claims would appear to be contrary to patent law or to copyright law which does the same for works available to the public, or to contract law which requires informed knowing assent to reasonable contract terms as a condition of enforceability in court. Only if all such covered matters are trade secrets would many such clauses appear sustainable, but even so a condition of trade secrecy is maintenance of the secret by the holder. This may not be met in the case of a widely distributed product offered for sale to anyone.

The legal status of such claims is uncertain. In the US, only two states have adopted a new revision of the Uniform Commercial Code which authorize such licensing restrictions, with disclosure after purchase. The validity of such terms remains uncertain. In the UK, Regulation 9 of the Electronic-Commerce (EC Directive) Regulations 2002 (SI 2002/2013) requires that a purchaser is able to determine in advance "the different technical steps to follow to conclude the contract"

C. WHAT IS CRYPTOGRAPHIC SIGNATURE

An electronic signature may incorporate a digital signature if it uses cryptographic methods to assure, at the least, both message integrity and authenticity. For example, a proposed contract accepted by a vendor and returned via email to the purchaser after being digitally signed. In fact, in modern practice, a digital signature of some text is always electronically processed in some sense, for the cryptographic mechanisms are impracticable without computers. In theory however, this is not required. Because of the use of message integrity mechanisms, any changes to a digitally signed document will be readily detectable if tested for, and the attached signature cannot then be taken as valid.

It is important to understand the cryptographic signatures are much more than an error checking technique akin to checksum algorithms, or even high reliability error detection and correction algorithms such as Reed-Solomon. These can offer no assurance that the text has not been tampered with, as all can be regenerated as needed by a tamperer. In addition, no message integrity protocols include error correction, for to do so would destroy the tempering detection feature.

Popular electronic signature standards include the OpenPGP standard supported by PGP and GnuPG, and some of the S/MIME IETF standards. All current cryptographic digital signature schemes require that the recipient have a way to obtain the sender's public key with assurances of some kind that the public key and sender identity properly belong together, and that message integrity measures (also digital signatures) which assure that neither the attestation nor the value of the public key can be surreptitiously changed. A secure channel is not typically required.

A digitally signed text may also be encrypted for protection during transmission, but this is not required when most digital signature protocols have been properly carried out. Condentiality requirments will be the guiding consideration.

D. ELECTRONIC SIGNATURE VS DIGITAL SIGNATURE

1. A Traditional Signing Process
2. Digital Signatures process
3. Electronic Signatures Process
4. Electronic Approval Management
5. Electronic Process Signature

The Electronic Signatures in Global and National Commerce Act (E-SIGN) officially gave electronic signatures the same legal standing as handwritten pen and paper ones. Digital Signature and Electronic Signatures have all been used interchangeably. The technologies inherent to each are actually sub-sets of one another, not their equivalent.

1. A Traditional Signing Process : Typically, a paper-based signing process being like this: People create a document in the most appropriate software application – such as

1. Word is ideal for straight text like legal contracts,
2. Excel works for budgets,
3. Form packages like Form Flow handles sectional forms as in an application or claim, and
4. XHTML is used for Web forms.

Then they apply their signatures. It is simple enough. But the meaning behind that signature is quite significant. That signature illustrates consent and identifies the signer. The ink permanently binds the signature to the paper so that it's virtually impossible to remove it.

The factors are

1. the foundation of the legal requirements for signing, and
2. in a court of law, that signature makes for a legally enforceable contract.

But most business processes require much more than a single signature. More often people are asked to fill in their name, add the date, and the city they've signed in. Even more complicated are the times that a document needs to be sent to other signatories for additional signature approvals. In the cases of sectional forms, as in an insurance claim or mortgage application, it gets particularly tricky as each person has to add information into their respective section, and then sign.

With these kinds of complex signing processes at work in most organizations today, making the shift from paper to electronic methods comes up against some roadblocks. It doesn't help matters either that what people expect, and what they actually get, from various products on the market often differ as drastically as the signing processes they're trying to move on-line in the first place.

2. Digital Signatures process: A digital signature certainly lends the impression that it produces an electronic version of handwritten signature, digital signature technology is actually the core technology used by many authentication solutions.

Digital signature technology doesn't come anywhere near emulating a legally binding signing act, not to mention a real-world approval process. Digital signatures encrypt data identify who did the encryption, and then validate and detect whether changes have been made. Contrary to what most people expect, a digital signature alone doesn't display an image of signature or a mark to illustrate consent regarding a document, nor is it part of the document at all. The digital signature is often linked to a document by a database application that a company typically creates to store it.

Digital signature is more complicated. To reproduce a signing process, it requires three signatures in a sectional form with digital signature technology, it requires storing three separate documents containing the three different data with their corresponding signatures. Digital signature technology requires that a software application be developed to produce a real-world signing process. That said digital signature technology is a sub-set of electronic signature technology which has greater functionality.

3. Electronic Signatures Process: Digital signature technology still does what it does best when someone signs with an electronic signature: encrypts the data and detects if changes have been made. Electronic signatures produce what digital signature technology stops. It actually displays an image of handwritten signature or a visual mark within the document to illustrate the writer's consent towards a document's contents and uniquely identify writer as a signer. In addition, it's permanently attached to a document – just like handwritten, pen-inked signature would be in a traditional, paper-based signing act.

Though, electronic signatures only really work for documents requiring a single signature. Unlike a paper-based model, where the second signer in an approval chain can make authorized changes to a document and take responsibility for the changes, or add information to his respective section of a document without invalidating the process, electronic signature technology would invalidate the first signature. That's because the technology doesn't recognize the content of signed data and is programmed to detect any all 'changes' made to the document by subsequent signers.

Use electronic signature technology alone to reproduce a multiple signature, sectional signing process and you'll have to start the signing process all over again and recreate the document form from scratch if

you don't want each signature to appear twice. This is when the heightened security provided by electronic signature technology falls short of its promise.

4. Electronic Approval Management: A digital signature technology is a subset of electronic signature technology and an electronic signature technology is a subset of its own accord, this time, of electronic approval management technology. Electronic approval technology is a solution that duplicates the same process follows in a traditional, business process.

Electronic approval management solutions have appropriated the nuances of real-world approval processes as closely as possible. It duplicates a legally binding signing process by visibly displaying our signature and demonstrating your consent towards a document's content, and allows separate people in an approval chain to add information to their respective sections and signing their names just like they would on paper.

Electronic approval management solutions recognize content and intelligently authenticate what each person has signed and are responsible for. This allows multiple signatures to be added to a document, additions and modifications to be made, and the same kind of signing flexibility you'd find with paper. And for heightened security, should someone tamper accidentally or maliciously with a document or attempted fraudulent use of the signatures contained therein, it visibly invalidates the electronic signatures.

5. Electronic Process Signature: An Electronic Process Signature is a new form of electronic signature technology developed by Silanis for Web-based transactions and electronic document automation. It captures and stores the entire web sequence of events and content involved in a transaction including the review, signing, acceptance and delivery of documents. The resulting stored Electronic Evidence is linked to the final transaction documents that have signed and/or delivered by an electronic document automation system. The Electronic Evidence can then be used to reliably and accurately reproduce the transaction exactly as it occurred and demonstrate compliance in legal, regulatory or internal proceedings.

The Electronic Process Signature technology can be used with any form of electronic signature in a web-based application to create its Electronic Evidence. This includes Zero-client click-through, holographic signature capture devices, and digital certificates and credentials.

Chapter–19
Cyber Vandalism

1. What is Vandalism:

Vandalism means willful wanton and malicious destruction of the property of others. It is the conspicuous defacement or destruction of a structure, a symbol or anything else that goes against the will of the owner / governing body, and usually constitutes a crime. Historically, it has been justified by painter Gustave Courbet as destruction of monuments symbolizing war and conquest.

Therefore, vandalism is often done as an expression of contempt, creativity, or both. Vandalism is only a meaningful concept in a culture that recognizes history and archaeology. Like other similar terms Barbarian / barbary, and Philistine, the term Vandal was originally an ethnic slur referring to the Vandals, who under Geiseric sacked Rome in 455. The Vandals, like the Philistines, no longer exist as an identifiable ethnic group.

The term vandalism in its modern acceptance was coined in January 1794 during the French Revolution, by Henri Grégoire, constitutional bishop of Blois. In Republican Convention, he used word Vandalism to describe some aspects of the behaviour of the republican army.

During the 1871 Paris Commune, Gustave Courbet's attempt, to dismantle the Vendôme column. It was a symbol of the past Napoleon III authoritarian Empire. It was one of the most celebrated

events of vandalism. As the Vendôme column is formally considered a monument devoid of any artistic value, tending to perpetuate with its expression ideas of war and conquest of the past imperial dynasty, that are reprobated by a republican nation's sentiment, citizen Courbet is to emit his wish that the National Defense government will allow him to dismantle this column.

Nietzsche himself would meditate after the Commune on the fight against culture. He take it as example of the intentional burning of the Tuileries Palace on May 23, 1871. The criminal fight against culture is only the reverse side of a criminal culture wrote Klossowski after quoting Nietzsche.

The destruction of glass windows and doors is a common form of vandalism. Bus seats are often an easy target for tag vandalism. Though vandalism in itself is illegal, it is often also an integral part of modern popular culture.

2. Cybervandalism or Webvandalism:

Cyber or Web vandalism is an attacks that deface webpages, or denial-of-service attacks. This is normally swiftly combated and of little harm.

3. What is Cyber counter-intelligence?

Cyber counterintelligence are measures to identify, penetrate, or neutralize foreign operations. It use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

4. When Vandalism is a crime

Private citizens commit vandalism when they wilfully damage or deface the property of others or the commons. Some vandalism qualifies as culture jamming or sniggling. It is artistic in nature as well as being carried out illegally or without the property owner's permission. Examples include at least some graffiti art, billboard liberation and possibly crop circles. Criminal vandalism has any of the three forms, Such as-

a. **Graffiti on public property** is common in many inner cities as part of a gang culture,

b. **Devastating forms** are those involved with public unrest, such as rioting,

c. **Involve the wilful destruction of public and private property.** Vandalism per se is often considered one of the least serious common crimes. But it can become quite serious when committed extensively, violently or as an expression of hatred and intimidation.

5. Examples of vandalism

In the case of vandalism to private property, the owner (the victim), may feel that they were specifically targeted by the perpetrator. Such crime may be the wilful destruction of a car window. It is the perpetrator's a few seconds of entertainment, with no consideration, for the detriment and inconvenience of the victim.

Opportunistic vandalism may be filmed, the mentality of which can be akin to happy slapping. The large scale prevalence of gang graffiti in some inner cities has almost made it acceptable to the societies. It may go unnoticed, or not be removed. Because it may be a fruitless endeavour, to be graffitied on once again.

6. Punishment for vandalism

a. In Singapore a person who attempts to cause or commits an act of vandalism may be liable to imprisonment for up to 3 years and in conjunction may be punished with caning.

b. The act of vandalism in UK is construed as an environmental crime and may be dealt with an ASBO (Anti-Social Behavior Order).

c. Former New York City mayor Rudolph Giuliani made a crackdown on vandalism a centerpiece of his anti-crime agenda in the 1990s. A strong campaign against nonviolent quality of life, crimes such as vandalism would cause a corresponding decrease in violent crime.

Tags, designs, and styles of writing are commonplace on clothing and are an influence on many of the corporate logos with which we are familiar. Many skateparks and similar youth-oriented venues are decorated with commissioned graffiti-style artwork, and in many others patrons are welcome to leave their own. There is still, however, a very fine line between vandalism as an artform, as a political statement, and as a crime. An excellent example of one who walks this threefold line is Bristol born guerrilla-artist Banksy, who is revered as a cult artistic figure by many, but seen by others as a criminal.

Chapter–20
Cyber Chat or Chatting

Cyber Chat or Chatting

a. **Internet Relay Chat (IRC)**
b. **HTML chat**
c. **Instant messaging**
d. **Visual Chatrooms**
e. **Chat room activities**
f. **Rules of chatroom behavior**
g. **Web chat sites**
h. **Voice chat**
i. **Voice over Internet Protocol (VoIP)**
j. **Live Support Software**
k. **Online discussion**
l. **Online discourse environments**
m. **Chat groups**
n. **Hosted Chat**
o. **Webcam**

Cyber Chat or Chatting

The ward chat means an informal conversation. Online chat can be referred to any kind of communication over Internet. It is primarily meant to refer to direct one-on-one chat or text-based group chat which is formally known as synchronous conferencing.

The Internet's are offering well-known services online chat and messaging services for free. Most of the Internet service providers are beginning to show strong revenue streams from for-pay services. The adult service providers are profiting from the advent of reliable and high-speed broadband that are at the forefront of the for-pay online chat revolution.

There are countless web users replacing traditional conversational means with online chat and messaging. E-mail has

reduced the need for and usage of letters, faxes, and memos. Online chat is steadily replacing telephony as the means of office and home communication. The early adopters in these areas are undoubtedly teenage users of instant messaging. It might not be long before SMS text messaging usage declines as mobile handsets provide the technology for online chat.

A chat room or chatroom is a term used primarily by mass media to describe any form of synchronous conferencing, occasionally even asynchronous conferencing. The term can thus mean any technology ranging from real-time online chat over instant messaging and online forums to fully immersive graphical social environments.

a. Internet Relay Chat (IRC)

Online chat is a way of communicating by sending text messages to people in the same chat-room in real-time. The oldest forms of true chat rooms are the text-based variety. The most popular of this kind is Internet Relay Chat (IRC). However, there are also talkers and havens. The popularity of these kinds of chat rooms have waned over the years, and IRC's popularity has rapidly given way to instant messaging. Also a notable number of people were introduced to chat rooms from AOL and web chat sites. There are also graphical user interface (GUI) text-based chat rooms which allow users to select an identifying icon and modify the look of their chat environment.

b. HTML chat

The HTML chat system is also very useful. It only requires having access to internet. It does not require any Java applet to be installed or any chat software like mIRC, etc. The simplest example of the HTML-based chat systems is CGI IRC chat.

c. Instant messaging

Instant messaging may not be truly chat rooms as they are characterized by being one on one conversation with people in a users buddy list. These systems have also started to incorporate the ability to chat with multiple people simultaneously. But these are still conversations restricted to the user's buddy list, not a group style venue.

d. Visual Chatrooms

Visual chat rooms add graphics to the chat experience. These are characterized by using a graphic representation of the user that can be

moved about a graphic background or in a graphic environment. These virtual worlds are capable of incorporating elements such as games and educational material most often developed by individual site owners, who in general are simply more advanced users of the systems. The most popular environments also allow users to create or build their own spaces. Some visual chat rooms also incorporate audio and video communications so that users may actually see and hear each other.

e. Chat room activities

The use of a chat room is to share information via text with a group of other users. New technology has enabled the use of file sharing and webcams to be included in some programs and almost all Internet chat or messaging services allow users to display or send to each other photos of themselves. Some people use chat rooms as a place to experience online sex, also known as cybersex or computer love. They are not physically able to see their partner. Cyber-ers apparently get stimulation by reading x-rated quotes. It is important that the partakers in such activities do not reveal personal information such as addresses as sexual predators may use cybersex as a tool to stalk chatroom users. Games are also often played in chat rooms. Historic examples are initgame, Hunt the Wumpus on IRC or an AOL chatroom game in AOL chat rooms. But the true use of a chat room is still to meet old and new people. Chat rooms are also used by pedophiles to groom children in order to abuse them.

f. Rules of chatroom behavior

Chat rooms usually have stringent rules that they require users to follow in order to maintain integrity and safety for their users. Particularly in rooms for children, rules usually do not allow users to use offensive language, or to promote hate mail, violence and other negative issues. Also chat rooms often do not allow advertising in their rooms or flooding, which is continually filling the screen with repetitive text. Typing with caps lock on is usually considered shouting and is discouraged. Chat rooms usually have a list of rules for users to obey when they chat online.

Sometimes chat room venues are moderated either by limiting who is allowed to speak, or by having moderation volunteers patrol the venue watching for disruptive or otherwise undesirable behavior. Most commonly chat rooms are not moderated and users may type what they

personally choose to send. Chatrooms are an honest (not always positive) comparison to real life public activities.

g. Web chat sites

Web chat sites are websites that allow users to communicate in real time using easily accessible web interfaces. These types of internet chat rooms can be distinguished by their simplicity and accessibility to users. There are user-oriented web sites, such as discussion forums and social networking sites, web chat sites. This trait allows them to offer users instantaneous access, but also generates an extremely high level of competition between chat sites. There are hundreds of chat sites, which actively compete with each other to the point where some of the more popular ones actually censor the names of other chat sites, preventing users from referring each other to competing chats.

h. Voice chat

Voice chat is a modern form of communication used on the Internet. Voice chat has led to a significant increase in distant communications where two or more people from opposite ends of the world can talk almost free of cost. These included individual voice chat with another person, as well as conference call type voice chat facilities. Many video games with online multiplayer allow players to communicate via voice chatting. Some website allowed voice chatting with a headset. An online multiplayer service was released, making it to allow voice chatting through microphone.

i. Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is the routing of voice conversations over the Internet or through any other IP-based network. This can be done through IP Telephony, Internet telephony, Broadband telephony, Broadband Phone and Voice over Broadband etc. Companies providing VoIP service are commonly referred to as providers, and protocols which are used to carry voice signals over the IP network are commonly referred to as Voice over IP or VoIP protocols.

j. Live Support Software

Live Support Software is a popular term for instant messaging applications designed specifically to provide online assistance to users of a web site. The software enables the administrator or webmaster of a

web site to receive and respond to text communication from multiple users of the web site. The majority of live support applications opens in a window and connects the user to a member of call centre staff. The more advanced scripts allow the users to be queued, so that one member of staff can deal with a customer and then automatically move on to the next customer. The customer's position in the queue is sometimes displayed.

k. Online discussion

Online discussion is a form of computer networks communication. Online discussion groups tend to have a social element to them similar to a clique. There are generally established leaders as well as more and less frequent communicators. Additionally, a discussion of the social properties of online discussion would not be complete without mention of the internet troll. These social networks can be very dynamic can contain many thousands of members.

l. Online discourse environments

Online discourse environments are online spaces where people interact with one another by some means of discourse. This can include asynchronous discussion boards, synchronous chat, multi-user online games, or any other computer-mediated communication tool. These environments are primarily text-based. But they may contain multi-media elements such as images, animation, or emoticons. Research on online discourse often takes a social-cultural or linguistic view, where learning occurs through participation in computer-mediated communication (CMC).

m. Chat groups

Chat groups are websites that allow users to communicate in real time using easily accessible web interfaces. They are types of internet chat rooms distinguished by their simplicity and accessibility to users who do not wish to take the time to install and learn to use specialized chat software. Unlike other user-oriented web sites, such as discussion forums and social networking sites, web chat sites typically do not require registration. This trait allows them to offer users instantaneous access, but also generates an extremely high level of competition between chat sites, as it allows users to switch between them with ease. There are hundreds of chat sites, which actively compete with each other to the point where some of the more

popular ones actually censor the names of other chat sites, preventing users from referring each other to competing chats.

n. Hosted Chat

Hosted Chat or Chat As Service is an ASP (Application Service Provider) model text chat service that boasts capabilities such as having multiple instances of a chat with different configurations being distributed among websites, blogs, discussion groups, and virtually every other type of online community.

o. Webcam :

A web camera or webcam is a real-time camera (usually, though not always, a video camera) whose images can be accessed using the World Wide Web, instant messaging, or a PC video calling application. The term webcam is also used to describe the low-resolution digital video cameras designed for such purposes, but which can also be used to record in a non-real-time fashion.

Chapter–21
Short Notes

1. Cyber Defamation

Cyber Defamation occurs when defamation takes place with the help of computers and the Internet. As for example someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

In a recent occurrence, 'A' a young girl was about to be married to 'B'. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant. Then, one day when she met 'B', he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about 'A's character. Some of them spoke of affairs, which she had had in the past. He told her that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, 'B' was able to prevail upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails.

During investigation, it was revealed that the person sending those e-mails was none other than 'A's stepfather. He had sent these e-mails so as to break up the marriage. The girl's marriage

would have caused him to lose control of her property of which he was the guardian till she got married.

Another famous case of cyber defamation occurred in America. All friends and relatives of a lady were beset with obscene e-mail messages appearing to originate from her account. These mails were giving the lady in question a bad name among her friends. The lady was an activist against pornography. In reality, a group of people became displeased with her views and angry with her for opposing them. They had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene e-mails they also put up websites about her. That basically maligned her character and sent e-mails to her family and friends containing matter defaming her.

2. (A) Cyber crime & (B) Cyber Financial crime

A. Cyber crime :

Cyber crime can differentiate from conventional Crime. Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, financial crimes and all of which are subject to the Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the (Indian) Information Technology Act, 2000. The computer network is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers.

Cyber crimes can be defined as acts that are punishable by the Indian Information Technology Act 2000. It would be also unsuitable as the Penal Code applicable in Bangladesh as well as Bangladesh Information technology Act 2005. It covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc.

Cyber crime can be defined as, **"Cyber crime is an unlawful act using computer network as a tool or a target or both among the Net-nationality with in the cyber space."**

B. Cyber Financial crime :

Financial Crimes are defined as a crime against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit. Financial crimes often involve fraud.

Financial Crimes are carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud,

payment fraud, currency fraud, and health care fraud. They involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering. Financial crimes sometimes, but not always, involve criminal acts such as elder abuse, armed robbery, burglary, and even murder. Victims range from individuals to institutions, corporations, governments and entire economies.

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.

Mortgage fraud is a term used to describe a broad variety of actions where the intent is to materially misrepresent information on a mortgage loan application, in order to obtain the loan. Mortgage fraud is not to be confused with predatory mortgage lending. Mortgage fraud is when one or more individuals defraud a financial institution; predatory lending is when a dishonest financial institution willfully misleads or deceives the consumer.

3. Cyber pornography crime

Cyber pornography includes followings:

1. Pornographic websites;
2. Pornographic magazines produced using computers to publish and print the material.
3. The Internet to download and transmit pornographic pictures, photos, writings etc.

As an example of Cyber pornography can be mentioned the Indian incidents "Air Force Balbharati School case." A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting ser ice. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken. In another incident, in Mumbai a

Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai police arrested the couple for pornography.

4. Cyber stalking or Cyber harassment crime

The Oxford dictionary defines stalking as 'pursuing stealthily'. Cyber stalking involves a person's movements across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim and constantly bombarding the victim with emails etc.

Cyber stalking or Cyberharassment is the electronic manifestation of physical stalking. It can be manifested through harassing e-mails, impersonating someone online, creating hate websites, posting harassing messages on message boards or abusive behavior in chat rooms. It is not just one event but an ongoing process that threatens or makes that person feal scared. Someone who does this is called a stalker. The stalker may do this because they want to be invovled in that person's life or because they want to have power over that person's life. The stalker can hurt that person's feelings by making them scared. They may feel they do not have the power to stop the stalker. Psychologists say stalking is a way of hurting someone's mind with serious effects. Sometimes a stalker may go on to hurt that person's body by assaulting, raping or murdering that person. The majority of online victims are female.

The staiker uses the internet to contact or follow that person. The stalker may make direct contact with that person, they may send nasty messages to that person or spread lies about them to others. Sometimes stalkers use the internet to learn more about the other person. They might find their address, phone number, workplace or photograph. Then they might use this information to do more stalking or find other ways to hurt that person on the internet or hurt their body.

Bad effect on society from Cyber Stalking

In 1993 there were 5000 websites on the Internet and today there are billions. Many of the websites devoted exclusively to pornography and many websites run by pedophiles. Chat rooms are frequented by a variety of people, including children who are restless and women who are looking for companionship. Both are easy targets for the cyber-predator.

In many cases, child molesters enter chat rooms pretending to be children. These molesters have perfected the art of cyber-stalking. They set up a meeting, and before the child realizes it, he is abducted. The Internet allows predators to deceive others and pretend they are something. Since image is everything on the Internet, people on chat rooms can live in a fantasy world.

Most cyberstalking appears to be committed by strangers given the vast number of sexual predator, celebrity, and nuisance stalkers currently using the Internet. The stalking landscape will continue to fluctuate as more individuals from all socioeconomic statuses, ethnic / racial backgrounds, political persuasions, and religious belief systems embrace the ether world.

Pedophiles prefer the company of children both socially and emotionally. Many pedophiles work in adult settings. They always prefer the company of children. They usually are not married and live alone or with a relative. Their fantasies involve being emotionally attached. They may physically involve with a child. The pedophile does not actually seek out children but instead uses movies, props, photographs, etc., to fulfill fantasies and sexual desires. The aggressive pedophile seeks out children for sexual purposes, including murder.

The child molester prefers children. They are likely to be married and have a family. The key distinguishing factor is sexual contact with children. Once the pedophile begins to approach children, he is no longer in a benign status engaged in only sexual fantasies involving children. Pedophiles and child molesters can be found affiliated with NAMBLA (North American Man-Boy Love Association), Free Spirits, the Renee Guyon Society, Pedophile Liberation Front and other organizations.

Internet chat rooms, especially those designed for younger persons, have become virtual playgrounds for sexual predators. Pedophiles who may have kept their fantasies to themselves now have a forum to discuss their thoughts with other pedophiles as well as daily opportunities to visit chat rooms and begin relationships with unsuspecting victims.

An example: In California, a 60-year-old ophthalmologist contacted a 13-year-old girl and after a few e-mail exchanges began sending her sexually explicit photographs. Eventually the doctor asked to meet the

obtain permission from the copyright holder. Nowadays the technology has changed. Today the Copyright law encompasses not only those forms of traditional expression understood as writings, but also include architectural designs, works of graphic art, motion pictures, audio and video recordings, and computer software etc.

b. What is Copyright security :

Copyright security is the protection and measures taken to prevent the unauthorized duplication of copyrighted materials. Modern societies are digitalized and computerized. To Maintain and to protect copyright security high-tech Software is used. Copyright holders often take extraordinary measures, including the retention of detective agencies, to police acts of copyright infringement.

Computer software security refers to the use of software to prevent damage to computer files, programs, and operating systems, as well as to monitor a personal computer (PC) or laptop for theft. Anti-virus software a recommended feature for any computer that is connected to the Internet is the software that protects the computer from viruses. Like biological viruses, computer viruses need the machinery of another host, in this case a computer, to make new copies of them and infect another host computer.

c. What is Data encryption and ownership :

Encryption is the scrambling of the data so as to make the data undecipherable. Encryption programs can scramble the data that is resident in the computer as well as data sent to another computer via email. The message can be reassembled to the original format if the receiving computer has an encryption program installed. With contracts being sent over the Internet, the ownership and legal status of such information has become an important issue. Digital signatures can be affixed to a document sent via the Internet to establish ownership, in the same way that a signature on a paper contract is legally binding.

d. What is Authorization and intrusion :

Software programs allow a hierarchy of approvals to be established for access to data. In a company, for example, senior managers can be authorized to view and even manipulate data that more junior personnel do not have access to. Other programs act as guardians of the data, and detect any unauthorized or unusual actions on the computer (i.e., hacking).

Computers connected to the Internet are often equipped with software known as a firewall. The firewall functions to monitor incoming transmissions and to restrict those that are deemed suspicious. It is a controlled gateway that limits who and what can pass through. A number of vendors offer firewall programs. Like anti-virus software, these programs can and should be frequently updated, since those who seek to maliciously gain remote access to computers are constantly developing methods to thwart the firewall barrier.

e. What is Copy right law :

Copyright law is the law that protects the exclusive right of copyright holder. To protect a copyright, the work must be original, and must be in a concrete medium. A work need not carry a copyright notice to be copyrighted, nor is registration required. However, copyright holders may obtain registration

The DMCA (The Digital Millennium Copyright Act) endures criticism from detractors who consider it as squelching the free exchange of ideas through the Internet and electronic media. Although controversial, the DMCA remains law, and as such requires enforcement. In addition to law enforcement agencies, clientele includes private holders of intellectual property who pay the company to protect that property against infringements in cyberspace. These electronic files may include software, audio, video recordings in digital format, or other materials.

IP or Internet Protocol address at which illegal activity is taking place, under the DMCA (The Digital Millennium Copyright Act.), it has the right to subpoena logs kept by the Internet service provider. These logs will enable it to connect IP addresses with user accounts. Arrest of lawbreakers may follow, depending on the seriousness of the crime and the degree of desire for enforcement on the part of the client. Legal issues involving the Internet are potentially broad. Any legal issues involving information technology is related to intellectual property issues

f. What is Intellectual Property Cyber crime :

Intellectual Property crimes include the following:

1. Software piracy,
2. Copyright infringement,

3. Trademarks violations,
4. Theft of computer source code etc.

g. What is Valuation of intellectual property (IP) :

The principle of valuing IP is to determine the future income associated with its ownership (Smith & Parr: Valuation of Intellectual Property and Intangible Assets, 3rd Edition, Wiley 2000). The value of IP is generally independent of its cost. Determination of future income requires estimating the income due to the IP in each of all future years over its life; i.e., the amount sold and the net income per unit after routine sales costs are deducted. If the IP is used internally, then the savings due to owning it can be similarly estimated. The risk that intellectual property becomes obsolete is high, and reduces the current value. Without risk, future income is discounted by using a risk-free interest rate. Risks include unexpected competition, unauthorized copying, patent breaches or invalidation, and loss of trade secrets. With such risks, discount rates increase, based on the expected Beta coefficient. With high discount rates, sales that occur far in the future have little effect, simplifying the determination of the net current value of the included IP.

When the items being valued contain multiple IP components, then the proportion and life of each component must be determined. That case exists in the small, as for software that receives updates throughout the future, and in the large, for companies that vend many products. Shareholders of public companies in effect estimate the aggregate IP of a company, providing a market capitalization through the price they are willing to pay for shares, which is in effect the sum of the book value and the IP owned by the company.

h. Intellectual property rights in the digital era :

Intellectual property rights (IPRs) in the digital era have added a new dimension to the traditional regime of IPRs. The complexity and jurisdictional issues relating to the Internet are challenging the IPR regime drastically. Though, TRIPS Agreement has tried to harmonies the IPRs all over the world yet the digital issues are vexing the IPRs enforcement everywhere. There is no harmonized law vis-à-vis IPRs in the digital era and this gives rise to conflict of laws. At the same time certain technological measures have also been adopted to tackle the

violations of IPRs in the digital environment but their efficiency and effectiveness is doubted.

Natural law or the law of nature (Latin: lax naturalis) is an ethical theory that posits the existence of a law whose content is set by nature and that therefore has validity everywhere. The phrase natural law is sometimes opposed to the positive law of a given political community, society, or nation-state, and can thus function as a standard by which to criticize that law. In natural law jurisprudence, on the other hand, the content of positive law cannot be known without some reference to the natural law. Natural law can be used synonymously with natural justice or natural right (Latin ius naturale), although most contemporary political and legal theorists separate the two.

Natural law theories have exercised a profound influence on the development of English common law, and have featured greatly in the philosophies of Thomas Aquinas, Francisco Suárez, Richard Hooker, Thomas Hobbes, Hugo Grotius, Samuel von Pufendorf, and John Locke. Because of the intersection between natural law and natural rights, it has been cited as a component in United States Declaration of Independence.

6. E-mail abuse:

What is E-mail : Electronic mail is abbreviated as e-mail or email. It is a method for composing, sending, storing, and receiving messages over electronic communication systems. The term e-mail applies both to the Internet e-mail system based on the Simple Mail Transfer Protocol (SMTP) and to intranet systems allowing users within one organization to e-mail each other. Often these workgroup collaboration organizations may use the Internet protocols for internal e-mail service

What is E-mail abuse : E-mail abuse takes place in many forms, such as:

1. Unsolicited commercial e-mail,
2. Unsolicited bulk e-mail,
3. Mail bombs,
4. E-mail harassment,
5. E-mail containing abusive or offensive content.

7. Online gambling cyber crime

Online gambling are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

8. Password & Password Fraud

A password is a secret tool for the user and a form of secret authentication data that is used to control access to a resource. The password is kept secret by the user from those who are not authorised to access of his computer network etc. The password protects the unauthorized access and uses of the computer network. It also secured the right of the users The passwords have been using from ancient Roman times. Sentries guarding a location would challenge for a password. They would only allow a person in if they knew the password.

In modern times, passwords are used to control access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.

Passwords are not actual words and a desirable property of the user. The password is often used to describe what would be more accurately called a passphrase. Passcode is sometimes taken to imply that the information used is purely numeric, such as the personal identification number (PIN) commonly used for ATM access. Passwords are generally short enough to be memorized.

User in a computing context refers to one who uses a computer system. Users may need to identify themselves for the purposes of accounting, security, logging and resource management. In order to identify oneself, a user has an account (a user account) and a username (also called a screen name, handle, nickname, or nick on some systems), and in most cases also a password. Users employ the user interface to access systems, and the process of identification is often referred to as authentication.

Password Manager : A password manager is software that helps a user organize passwords and PIN codes. The software typically has a local database or files that hold the encrypted password data. Many

password managers also work as a form filler, thus they fill the user and password data automatically into forms. Some have password generator capabilities. In addition to stand-alone password manager applications, there are also web-based online password managers.

Password cracking : Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crack able passwords.

Fraud : In the broadest sense, a fraud is a deception made for personal gain. The specific legal definition varies by legal jurisdiction. Fraud is a crime, and is also a civil law violation. Many hoaxes are fraudulent, although those not made for personal gain are not technically frauds. Defrauding people of money is presumably the most common type of fraud, but there have also been many fraudulent discoveries in art, archaeology, and science. The John Cooke Fraud Report offers a three word fraud definition: "Gain Through Misrepresentation."

In criminal law, fraud is the crime or offense of deliberately deceiving another in order to damage them – usually, to obtain property or services unjustly. Fraud can be accomplished through the aid of forged objects. In the criminal law of common law jurisdictions it may be called "theft by deception," "larceny by trick," "larceny by fraud and deception" or something similar.

In academia and science, fraud can refer to academic fraud – the falsifying of research findings which is a form of scientific misconduct and in common use intellectual fraud signifies falsification of a position taken or implied by an author or speaker, within a book, controversy or debate, or an idea deceptively presented to hide known logical weaknesses. Journalistic fraud implies a similar notion, the falsification of journalistic findings.

Password Fraud : Password fraud is a Fraud that can be committed through many methods, including mail, wire, phone, and

the internet, computer crime and internet fraud by cracking password. Fraud, in addition to being a criminal act, is also a type of civil law violation known as a tort. A tort is a civil wrong for which the law provides a remedy

9. Sale of illegal articles cyber Crime

Sale of illegal articles would include sale of

1. Narcotics,
2. Weapons and wildlife etc.,
3. Posting information on websites,
4. Auction websites,
5. Bulletin boards or by using email communication.

10. What is Search :

According to law, **Search** is the examination of a person's premises (residence, business, or vehicle) by law enforcement officers looking for evidence of the commission of a crime. Searches and seizures must be under the authority of a search warrant or when the officer has solid facts that give him/her probable cause to believe that there was evidence of a specific crime in the premises and no time to get a warrant. Evidence obtained in violation of the Constitution is not admissible in court, nor is evidence traced through such illegal evidence

11. What is Seizure :

Seizure literally means, The act of forcibly dispossessing an owner of a property : The act of taking of a person by force : The taking possession of something by legal process.

According to law, **Seizure** is the taking (removal) of articles of evidence; such as controlled narcotics, a pistol, counterfeit bills, a blood-soaked blanket by law enforcement officers looking for evidence of the commission of a crime.

According to law a seizure is also the deprivation of liberty, or the enjoyment in exercising dominion or control over a thing. The thing may be property or person. Police can temporarily seize private property. This varies from jurisdiction to jurisdiction. Usually it can be hold indefinitely if it is material evidence in a criminal case. Temporary seizure or detention of a person is allowed for shorter periods of time.

Asset forfeiture laws apply to criminal cases, and among other things are intended to show that crime does not pay. Seized property can be auctioned off for money to fund the criminal justice system, or in some cases, used by the police departments themselves in operations.

12. Search & Seizure in Electronic evidence

Computers and the Internet have entered the mainstream of life. Millions of people spend several hours every day in front of computers, where they send and receive e-mail, search the Web, maintain data bases, and participate in countless other activities. Those who commit crime have not missed the computer revolution. An increasing number of criminals use pagers, cellular phones, laptop computers and network servers in the course of committing their crimes. In some cases, computers provide the means of committing crime. For example:

1. The Internet can be used to deliver a death threat via e-mail;
2. To launch hacker attacks against a vulnerable computer network;
3. To disseminate computer viruses; or
4. To transmit images of child pornography.

In other cases, computers merely serve as convenient storage devices for evidence of crime. For example, a money laundering operation might retain false financial records in a file on a network server.

The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers. Electronic records such as computer network logs, e-mails, word processing files, and ".jpg" picture files increasingly provide the government with important (and sometimes essential) evidence in criminal cases. Therefore search and seizure is required for the electronic investigation of a crime.

Chapter–22
E-Commerce & M-Commerce

---

1. What is E-commerce

E-Commerce denotes Electronic Commerce. It is exactly analogous to a marketplace on the Internet. Electronic Commerce also referred to as EC, e-commerce eCommerce or ecommerce.

It consists primarily of the distributing, buying, selling, marketing and servicing of products or services over electronic systems, such as the Internet and other computer networks. The information technology industry might see it as an electronic business application aimed at commercial transactions in this context. It can involve -

1. Electronic funds transfer.
2. Supply chain management.
3. E-marketing,
4. Online marketing,
5. Online transaction processing,
6. Electronic data interchange (EDI),
7. Automated inventory management systems, and
1. Automated data collection systems.

Electronic commerce typically uses electronic communications technology of the World Wide Web, at some point in the transaction's lifecycle. Electronic commerce generally depends upon computer technologies other than the World Wide Web, such as databases, and e-mail. and on other non-computer technologies, such as transportation for physical goods sold via e-commerce.

According to Person Halls book E-Commerce started in 1994 with the first banner ad being placed on a website. According to the October 2006 Forreste7r Research report entitled, US E-Commerce: Five-Year Forecast And Data Overview, "Nontravel online retail revenues will top the quarter-trillion-dollar mark by 2011. A segment of the most active Web shopping households that is roughly 8 million strong. This group of consumers is extremely comfortable with technology and values convenience above all else in the online retail experience. As retailers begin to wade through their copious data warehouses and understand the who, what, when, where, why, and how of this segment, they will benefit from targeting these customers.

2. Development of E-commerce

The meaning of the term Electronic Commerce has changed over the last 30 years. Originally, Electronic Commerce meant the facilitation of commercial transactions electronically, usually using technology like Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT). These were introduced in the late 1970s, for example, to send commercial documents like purchase orders or invoices electronically.

The 'electronic' or 'e' in e-commerce refers to the technology/systems; the 'commerce' refers to be traditional business models. E-commerce is the complete set of processes that support commercial/business activities on a network. In the 1970s and 1980s, this would also have involved information analysis. The growth and acceptance of credit cards, automated teller machines (ATM) and telephone banking in the 1980s were also forms of e-commerce. From the 1990s onwards, this would include Enterprise Resource Planning systems (ERP), data mining and data warehousing.

In the dot com era, it came to include activities more precisely termed "Web commerce". The purchase of goods and services over the World Wide Web, usually with secure connections HTTPS, a special server protocol that encrypts confidential ordering data for customer

protection) with e-shopping carts and with electronic payment services, like credit card payment authorizations.

Today, it encompasses a very wide range of business activities and processes, from e-banking to offshore manufacturing to e-logistics. The ever growing dependence of modern industries on electronically enabled business processes gave impetus to the growth and development of supporting systems, including backend systems, applications and middleware. Examples are broadband and fiber-optic networks, supply-chain management software, customer relationship management software, inventory control systems and financial accounting software.

When the Web first became well-known among the general public in 1994, many journalists and pundits forecast that e-commerce would soon become a major economic sector. It took about four years for security protocols (like HTTPS) to become sufficiently developed and widely deployed. Subsequently, between 1998 and 2000, a substantial number of businesses in the United States and Western Europe developed rudimentary web sites.

Large number of pure e-commerce companies disappeared during the dot-com collapse in 2000 and 2001, many "brick-and-mortar" retailers recognized that such companies had identified valuable niche markets and began to add e-commerce capabilities to their Web sites. For example, after the collapse of online grocer Webvan, two traditional supermarket chains, Albertsons and Safeway, both started e-commerce subsidiaries through which consumers could order groceries online.

E-commerce significantly lowered barriers to entry in the selling of many types of goods. Many small home-based proprietors are able to use the internet to sell goods. Often, small sellers use online auction sites such as EBay, or sell via large corporate websites like Amazon.com, in order to take advantage of the exposure and setup convenience of such sites.

3. What are the Success factors in e-commerce

a. Technical and organizational aspects
b. Customer-Oriented aspects of E-commerce
c. Problems of E-commerce
d. Product suitability in E-commerce
e. Disadvantages of e-commerce
f. Consumers Acceptance of E-commerce

g. Biggest Five Online E-Commerce Web Sites

h. Propular sites of Ecommerce News

a. Technical and organizational aspects of E-commerce

E-commerce company will survive not only based on its product, but by having a competent management team, good post-sales services, well-organized business structure, network infrastructure and a secured, well-designed website. Such factors include:

1. Sufficient work done in market research and analysis. E-commerce is not exempt from good business planning and the fundamental laws of supply and demand. Business failure is as much a reality in e-commerce as in any other form of business.

2. A good management team armed with information technology strategy. A company's IT strategy should be a part of the business re-design process.

3. Providing an easy and secured way for customers to effect transactions. Credit cards are the most popular means of sending payments on the internet, accounting for 90% of online purchases. In the past, card numbers were transferred securely between the customer and merchant through independent payment gateways. Such independent payment gateways are still used by most small and home businesses. Most merchants today process credit card transactions on site through arrangements made with commercial banks or credit cards companies.

4. Providing reliability and security. Parallel servers, hardware redundancy, fail-safe technology, information encryption, and firewalls can enhance this requirement.

5. Providing a 360-degree view of the customer relationship, defined as ensuring that all employees, suppliers, and partners have a complete view, and the same view, of the customer. Customers may not appreciate the big brother experience.

6. Engineering an electronic value chain in which one focuses on a "limited" number of core competencies -- the opposite of a one-stop shop. Electronic stores can appear either specialist or generalist if properly programmed.

7. Operating on or near the cutting edge of technology and staying there as technology changes (but remembering that the fundamentals of commerce remain indifferent to technology).

8. Setting up an organization of sufficient alertness and agility to respond quickly to any changes in the economic, social and physical environment.

9. Providing an attractive website. The tasteful use of colour, graphics, animation, photographs, fonts, and white-space percentage may aid success in this respect.

10. Streamlining business processes, possibly through re-engineering and information technologies.

11. Providing complete understanding of the products or services offered, which not only includes complete product information, but also sound advisors and selectors.

Naturally, the e-commerce vendor must also perform such mundane tasks as being truthful about its product and its availability, shipping reliably, and handling complaints promptly and effectively. A unique property of the Internet environment is that individual customers have access to far more information about the seller than they would find in a brick-and-mortar situation.

b. Customer-Oriented aspects of E-commerce

A successful e-commerce organization must also provide an enjoyable and rewarding experience to its customers. Many factors go into making this possible. Such factors include:

1. Providing value to customers. Vendors can achieve this by offering a product or product-line that attracts potential customers at a competitive price, as in non-electronic commerce.

2. Providing service and performance. Offering a responsive, user-friendly purchasing experience, just like a flesh-and-blood retailer, may go some way to achieving these goals.

3. Providing an incentive for customers to buy and to return. Sales promotions to this end can involve coupons, special offers, and discounts. Cross-linked websites and advertising affiliate programs can also help.

4. Providing personal attention. Personalized web sites, purchase suggestions, and personalized special offers may go some of the way to substituting for the face-to-face human interaction found at a traditional point of sale.

5. Providing a sense of community. Chat rooms, discussion boards, soliciting customer input and loyalty programs can help in this respect.

6. Owning the customer's total experience. E-tailers foster this by treating any contacts with a customer as part of a total experience, an experience that becomes synonymous with the brand.

7. Letting customers help themselves. Provision of a self-serve site, easy to use without assistance, can help in this respect. This implies that all product information is available, cross-sell information, advise for product alternatives, and supplies & accessory selectors.

8. Helping customers do their job of consuming. E-tailers and online shopping directories can provide such help through ample comparative information and good search facilities. Provision of component information and safety-and-health comments may assist e-tailers to define the customers' job.

c. Problems of E-commerce

A provider of E-commerce goods and services rigorously follows these "key factors" to devise an exemplary e-commerce strategy, problems can still arise. Sources of such problems include:

1. Failure to understand customers, why they buy and how they buy. Even a product with a sound value proposition can fail if producers and retailers do not understand customer habits, expectations, and motivations. E-commerce could potentially mitigate this potential problem with proactive and focused marketing research, just as traditional retailers may do.

2. Failure to consider the competitive situation. One may have the will to construct a viable book e-tailing business model, but lack the capability to compete with Amazon.com.

3. Inability to predict environmental reaction. What will competitors do? Will they introduce competitive brands or competitive web sites? Will they supplement their service offerings? Will they try to sabotage a competitor's site? Will price wars break out? What will the government do? Research into competitors, industries and markets may mitigate some consequences here, just as in non-electronic commerce.

4. Over-estimation of resource competence. Can staff, hardware, software, and processes handle the proposed strategy ? Have e-tailers failed to develop employee and management skills? These issues may call for thorough resource planning and employee training.

5. Failure to coordinate. If existing reporting and control relationships do not suffice, one can move towards a flat, accountable, and flexible organizational structure, which may or may not aid coordination.

6. Failure to obtain senior management commitment. This often results in a failure to gain sufficient corporate resources to accomplish a task. It may help to get top management involved right from the start.

7. Failure to obtain employee commitment. If planners do not explain their strategy well to employees, or fail to give employees the whole picture, then training and setting up incentives for workers to embrace the strategy may assist.

8. Under-estimation of time requirements. Setting up an e-commerce venture can take considerable time and money, and failure to understand the timing and sequencing of tasks can lead to significant cost overruns. Basic project planning, critical path, critical chain, or PERT analysis may mitigate such failings. Profitability may have to wait for the achievement of market share.

9. Failure to follow a plan. Poor follow-through after the initial planning, and insufficient tracking of progress against a plan can result in problems. One may mitigate such problems with standard tools: benchmarking, milestones, variance tracking, and penalties and rewards for variances.

10. Becoming the victim of organized crime. Many syndicates have caught on to the potential of the Internet as a new revenue stream. Two main methods are as follows: (1) Using identity theft techniques like phishing to order expensive goods and bill them to some innocent person, then liquidating the goods for quick cash; (2) Extortion by using a network of compromised "zombie" computers to engage in distributed denial of service attacks against the target Web site until it starts paying protection money.

11. Failure to expect the unexpected. Too often new businesses do not take into account the amount of time, money or resources needed to complete a project and often find themselves without the necessary components to become successful.

d. Product's suitability in E-commerce

Certain products or services appear more suitable for online sales; others remain more suitable for offline sales. Many successful purely virtual companies deal with digital products, music, movies, office supplies, education, communication, software, photography, and financial transactions. Examples of this type of company include: Google, eBay and Paypal. Other successful marketers such as use Drop shipping or Affiliate marketing techniques to facilitate transactions of tangible goods without maintaining real inventory. Examples include Amazing Refund and numerous sellers on eBay.

Virtual marketers can sell some non-digital products and services successfully. Such products generally have a high value-to-weight ratio, they may involve embarrassing purchases, they may typically go to people in

remote locations, and they may have shut-ins as their typical purchasers. Items which can fit through a standard letterbox are particularly suitable for a virtual marketer, and indeed Amazon.com, one of the few enduring dot-com companies, has historically concentrated on this field.

Products such as spare parts, both for consumer items like Blander Machine, Smoothing Iron, washing machines etc and for industrial equipment like centrifugal pumps, also seem good candidates for selling online. Retailers often need to order spare parts specially, since they typically do not stock them at consumer outlets. In such cases, e-commerce solutions in spares do not compete with retail stores, only with other ordering systems. A factor for success in this niche can consist of providing customers with exact, reliable information about which part number their particular version of a product needs, for example by providing parts lists keyed by serial number.

Purchases of pornography and of other sex-related products and services fulfill the requirements of both virtuality and potential embarrassment. Such services has become the most profitable segment of e-commerce.

e. Disadvantages of e-commerce

There are many disadvantages of e-commerce. One of the main disadvantage is fraud. The e-commerce users details (name, bank card number, age, national insurance number) are entered into what look to be a safe site but really it is not. These details can then be used to steal money from them and can be used to buy things online that users are completely unaware of until it is too late.

There are many problems with e-commerce some of which are:

1. Failure to understand customers: A product with a sound value proposition can fail if producers and retailers do not understand customer habits, expectations, and motivations. E-commerce could potentially mitigate this potential problem with proactive and focused marketing research.

2. Failure to consider the competitive situation: One may have the will to construct a viable book e-tailing business model, but lack the capability to compete with Amazon.

3. Inability to predict environmental reaction: Research into competitors, industries and markets may mitigate some consequences here, just as in non-electronic commerce. Over-estimation of resource competence. Can staff, hardware, software, and processes handle the proposed strategy? Have e-tailer's failed to develop employee and management skills? These issues may call for thorough resource planning and empioyee training.

4. Products less suitable for e-commerce include products that have a low value-to-weight ratio, products that have a smell, taste, or touch component, products that need trial fittings and products where colour integrity appears important. Tesco.com has had success delivering groceries in the UK, albeit that many of its goods are of a generic quality, and clothing sold through the internet is big business in the U.S. Also, the recycling program Cheapcycle sells goods over the internet, but avoids the low value-to-weight ratio problem by creating different groups for various regions, so that shipping costs remain low.

f. Consumers Acceptance of E-commerce

Consumers have accepted the e-commerce business model less readily than its proponents originally expected. Even in product categories suitable for e-commerce, electronic shopping has developed only slowly. Several reasons might account for the slow uptake, including:

1. Concerns about security. Many people will not use credit cards over the Internet due to concerns about theft and credit card fraud.

2. Lack of instant gratification with most e-purchases much of a consumer's reward for purchasing a product lies in the instant gratification of using and displaying that product. This reward does not exist when one's purchase does not arrive for days or weeks.

3. The problem of access to web commerce, mainly for poor households and for developing countries. Low penetration rates of Internet access in some sectors greatly reduces the potential for e-commerce.

4. The social aspect of shopping. Some people enjoy talking to sales staff, to other shoppers, or to their cohorts: this social reward side of retail therapy does not exist to the same extent in online shopping.

5. Poorly designed, bug-infested e-Commerce web sites that frustrate online shoppers and drive them away. Inconsistent return policies among e-tailers or difficulties in exchange/return.

g. Biggest Five Online E-Commerce Web Sites

1. Ebay.com
2. Yahoo.com
3. Amazon.com
4. Google.com
5. Buy.com

h. Popular site of Ecommerce News

1. E-commerce Guide

2. Ecommerce Best Practices (B2B)
3. Ecommerce Times
4. North American Consumer Project on Electronic Commerce (NACPEC)
5. Institute of Certified E-Commerce Consultants (ICECC)
6. eNewsline: eCommerce News for the Airline Industry
7. Internet Retailer
8. E-Commerce Ezine
9. E-Commerce Research Briefs
10. E-Commerce Law Blog

4. What is Mobile commerce (M-Commerce)

Mobile commerce denotes m-commerce. This is the new concept of technological development. Internet has changed perceptions, behaviors, societies and nations at large. It has changed the way we perceive, the way we interact and the way we do commerce. Internet has really enabled the making of electronic commerce as a practical reality.

The emergences of other technologies for example wireless technologies haye resulted in a new dimension for the applicability of electronic commerce. This is a new emergent field of Mobile Commerce or m-commerce. M-Commerce is a new method of commerce that takes place on and through the medium of wireless applications, sets, mobile phones and the like.

Mobile commerce is expected to be the dominant form of electronic commerce in the times to come, especially with the proliferation, growth and penetration of mobiles and other handheld devices. The adoption of Mobile commerce by large numbers of people would transform it into a practical mass revolution and reality.

The Mobile commerce is resulting in highly technical disputes, doubts and complicated questions of law. It has a direct bearing on the future growth of mobile commerce. The discipline of Mobile Commerce Law or M-COMMERCE LAW is the latest field of Cyberlaw. This is a highly specialized field of Cyberlaw. It is developing through out the world. Till today there has no uniformity of approach towards adoption of Wireless Application Protocol (WAP), as the universal mobile commerce technology platform and protocol.

5. E-Commerce in Bangladesh

Bangladesh is a developing country. Bangladesh is aware about the emergent power of Information Technology and Internet. E-commerce

is the demand of the modern technological era. So Bangladesh can not remain behind technological advancement.

Many Bangladeshi companies currently distribute their images through the Internet to clients all over the world. But the monetary transactions take place through conventional means. Some companies put messages on bulletin board, on ' internet yellow pages' with email links, and sometimes web pages, but there never is a place to submit a credit card. This is because currently the government does not permit credit card charges over the internet. The ISPs in Bangladesh do have the technology for e-commerce, and are anticipating governmental approval.

E-commerce sites needed to be hooked up to a merchant bank account. A merchant bank account allows a company to accept and process credit card transactions. All businesses that use electronic credit cards need to be hooked up to their merchant account. For example, in a grocery store, when one swipes a card through the card swipe machine, machine is hooked up to the grocery store's merchant account.

There are considerable numbers of private banks in Bangladesh. Most of the banks already have web pages. Most of these banks do offer online or electronic service such as Direct Deposit. Some of them have ATM machines, though not nearly as concentrated as in the United States. So online banking in Bangladesh started and developing day by day.

Asia is the fastest growing regional market in the world for information and communications services. The first GIIC Regional Meeting brought together senior government officials from 20 Asian economies, including Bangladesh, private sector business leaders, regional organizations, academics and technical experts to share experiences, and review best practices to help develop an information infrastructure to promote economic and social development in the region. The conference focused on the use of telecom and IT in health care and telemedicine, education and human resources development and the management of government services.

Bangladesh has accepted the obligations of Article VIII of IMF Articles of Agreement which means removal of all restrictions on making payments and transfers for current international transactions. By accepting these obligations, Bangladesh has given a clear signal to the international community that it would pursue sound economic policies, and thereby create a congenial climate for investment. Because of this potential influx of investment, one can only conclude that electronic payment systems are only a short breath away from becoming part of the Bengali way.

NGOs are on the web. For example Ikota Forum in Bangladesh is an NGO that represents 14 producer organizations that represent 75,000 women. They have a web site produced entirely in Bangladesh. The site shows many of the products, all of which were made by very poor people in remote rural settings in Bangladesh. Most other bigger NGOs have already gone on the web. Private Universities have already gone on the web.

E-Components: Power, Hardware, Communication

Bangladesh public power sector is inadequate. Overloading and lack of maintenance cause frequent outages and necessary planned blackouts. A country having inadequate power supply can not provide successful E-commerce. The Government has signed three agreements and Bangladesh began to purchase power from private companies.

Bangladesh has significant natural gas reserves. Due to inadequate gas transmission system, as well as electricity transmission system, is a bottleneck to growth in this area. The gas company has signed exploration and development agreements and aid is coming in from the ADB and World Bank. A new major gas pipeline built. In addition, transformers, wood poles, insulators, surge protectors, line tools and other parts needed for the electricity transmission system are being brought into the country.

The market for computer hardware peripherals is increasing day by day. Duties on imports were eliminated. This decreased prices of the computer and increases sales. Thus, hardware needed for e-commerce is coming within the reach of the users.

Bangladesh Telecommunication services are inadequate. The quality of the service is poor. Efforts are underway to upgrade it. There are plans for expansion of the domestic and international capacity. Analog exchanges are changing to digital. Private companies were allowed to enter into the market. Email and ISP providers are now mostly available. BTTB has proposed other upgrades in their services. Bangladesh already joined with the optical fiber super high way. It hosts communication cables so that e-commerce may one day live in Bangladesh.

Many companies have web sites where they market a product, but to purchase it buyer actually come into the store. This is because of the government's current restriction on e-commerce, which is expected to be resolved soon. Hotels that allow for internet booking are worldwide chains. The whole transaction occurs from outside of Bangladesh. These services should be extended to be performed in Bangladesh.

Chapter–23
E-Governance

1. What is E-Governance
2. Applicability of Law in E-Governance
3. E-Governance in Bangladesh
4. Aspects of E-governance in Bangladesh
   a. Technological Aspect
   b Human Resource Aspects
   c. Economic Aspects
   d. Social Aspects
   e. Administrative Aspects
   f. Legal Aspects
   g. Local Aspects
5. National strategy of E-Governance
   a. E-governance Awareness among public servants
   b. Facilitate public private partnership model to work
   c. Enhance access to ICT tools for citizens
   d. Creation of local content
   e. Adopt open standards and open source solutions
   f. Plan for the long term
6. E-governance initiatives in Bangladesh
   a. Automation of Internal Processes
   b. Electronic Birth Registration
   c. Financial Management
   d. Government Forms Online
   e. Hajj Web Site
   f. MIS for Project Management and Transparency
   g. National Board of Revenue
   h. Personnel Database
   i. Railway Ticketing
   j. Voter ID Card Preparation

1. What is E-Governance

According to Chamber's Dictionary, Governance literally means Government: control: direction: behaviour etc. So the term E-Governance means Electronic Governance. It is related with

1. Governments,
2. Civil society, and
3. Media

By using Information and Communication Technology (ICT) E-Governance can increase

1. Government accountability and
2. Government transparency

E-Governance can reduce

1. Corruption,
2. Increase citizen participation,
3. Improve financial management
4. Delivery of public services, and
5. Inform policy dialogue.

E-governance means using ICT strategically to strengthen democratic governance and to deliver customer-focused government services. E-Governance are designed to

1. Strengthen democratic government at all levels by improving the effectiveness, responsiveness, accountability, and transparency of institutions
2. Build the capacity of civil society to participate in the governing process
3. Support decentralization and democratic local governance
4. Help local governments share best practices and improve service delivery
5. Strengthen the advocacy role of municipal associations.

RTI is a partner in the USAID DOT-COM Alliance, which supports E-Governance initiatives, particularly in the areas of

1. Telecommunications,
2. E-commerce,
3. Internet policy, and
4. Regulatory reform.

The Role of ICT in Governance, may develop the problems that Governments facing are

1. Inefficiency,
2. Internal and external communications failures,
3. Poor service delivery, and
4. Corruption.

Civil society organizations are unable to use ICT effectively as a powerful tool for making information available to the public and preventing corrupt practices. ICT is to address real and urgent governance problems, particularly in building local government capacity. It can be done in the following way.

1. Deliver relevant applications and services to civil society and to local and national government institutions
2. Improve public access to information to improve government transparency and fight corruption
3. Provide access to essential information and improve processes encompassing education, culture, policy, regulation, infrastructure and public facilities
4. Help communicate and promote governance initiatives by working with community public opinion leaders and national media representatives, and
5. Share lessons learned and best practices.

2. Applicability of Law in E-Governance

Internet structure has raised several judicial concerns. Internet is independent of any geographic location. Individuals connect to the Internet and interact with others. It is possible for them to withhold personal informations and make their real identities anonymous. The laws that could govern the Internet, would be fundamentally diifferent from laws that geografic nations use today. David Johnson and David Post offer a solution to the problem of Internet governance. They stated that

"It becomes necessary for the Internet to govern itself. Instead of obeying the laws of a particular country, Internet citizens will obey the laws of electronic entities like service providers. Instead of identifying as a physical person, Internet citizens will be known by their usernames or email addresses. Since the Internet defies geographical boundaries, national laws will no longer apply. Instead, an entirely new set of laws

will be created to address concerns like intellectual property and individual rights. In effect, the Internet will exist as its own sovereign nation."

It is to be admitted that Internet should be regulated. Substantial regulation, both public and private, by many parties and at many different levels should be provided. There are five primary modes of regulation of the internet described by Lawrence Lessig in his book, Code and other laws of Cyberspace. These are given below:

a. Law:

"As the numerous statutes, evolving case law and precedents make clear, many actions on the internet are already subject to conventional legislation. Areas like gambling, child pornography, and fraud are regulated in very similar ways online as off-line. The determination of the most controversial and unclear areas of evolving laws has subject matter jurisdiction over activity conducted on the internet, particularly as cross border transactions affect local jurisdictions. It is certainly clear that substantial portions of internet activity are subject to traditional regulation. The conduct that is unlawful off-line is presumptively unlawful online, and subject to similar laws and regulations. Scandals with major corporations led to US legislation rethinking corporate governance regulations such as the Sarbance-Oxley Act."

b. Architecture:

"These mechanisms concern the parameters of the information can and cannot be transmitted across the internet. Everything from internet filtering software to encryption programs, to the very basic architecture of TCP / IP protocol, falls within this category of regulation. It is arguable that all other modes of regulation either rely on, or are significantly supported by, regulation via West coast Code."

c. Norms:

"Social interaction, conduct is regulated by social norms and conventions in significant ways. Certain activities or conduct through online may not be specifically prohibited by the code architecture of the internet, or expressly prohibited by applicable law. These activities or conduct will be invisibly regulated by the inherent standards of the community, called internet users. Certain conduct will cause an individual to be censored or self-regulated by the norms of community that one chooses to associate with on the Internet."

d. Markets:

"Markets also regulate certain patterns of conduct on the internet. Economic markets will have limited influence over non-commercial portions of the internet. The internet also creates a virtual marketplace for information. Such information affects everything from the comparative valuation of services to the traditional valuation of stocks. In addition, the increase in popularity of the internet as a means for transacting all forms of commercial activity, and as a forum for advertisement, has brought the laws of supply and demand in cyberspace."

e. Internet Regulation In different Countries

"In some United States law that does restrict access to materials on the internet, but does not truly filter the internet. Many Asian and Middle East nations use to block material that their governments have deemed inappropriate for their citizens to view. China and Saudi Arabia are two excellent examples of nations that have achieved high degrees of success in regulating their citizens access to the internet."

3. E-Governance in Bangladesh

The people republic of Bangladesh is an independent Country. It is governed by parliamentary form of Governments. It is a developing country and densely populated. Poverty, Illiteracy, corruption, efficiency, and transparency are the vital challenges in front of the Bangladesh Government.

The blessings of civilization, economic development and cultural achievement should be neutrally available for the every people of the country. Every citizen has their equal fundamental right as confirmed by the Constitution of the People Republic of Bangladesh. So the responsibility, efficiency and trusted management of the Government and its machinery are essential.

A good Governance and E-Governance can fulfill the Fundamental Principles of the State Policy. Information Communication Technology (ICT) is the blessings of modern scientific advancement. This technology can render its utmost endeavor for the fulfillment of the millennium century. Bangladesh is approaching towards that goal.

The government must deliver its services and in the long run, it must earn the confidence of the people by providing the services that people want. A properly designed and implemented E-

governance system has the potential to help government. In the Bangladesh context, the following can be the most direct gain that e-governance can bring to the country.

a. Transparency, Accountability and Efficiency:

E-governance provides the right tools for monitoring of the government activities by its citizenry by allowing the government to follow predefined and transparent processes whose quality and efficiency are measurable.

b. Decentralization of governance:

E-Government systems make decentralization of government services and makes decentralized decision-making easier.

c. Makes ICT relevant to the masses:

E-Government systems make ICT relevant to the masses as its benefits gradually extend to citizens and communities throughout the country.

d. Private sector development:

E-governance systems allow for easy accessibility to government services and allow businesses to access government services on the fly thereby enhancing overall competitiveness of enterprises in a country.

4. Aspects of E-governance in Bangladesh:

a Technological Aspect
b Human Resource Aspects
c. Economic Aspects
d. Social Aspects
e. Administrative Aspects
f. Legal Aspects
g. Local Aspects

a. Technological Aspect

Least Developed Countries are suffering from inadequacy of ICT infrastructure, is a common problem in most government offices of Bangladesh. This situation is further compounded by the marked absence of technical infrastructure planning and the inefficient utilization of infrastructure that is available.

The other challenge is in ensuring sustainability of ICT infrastructure. Often due to myopic planning of development projects, inefficiency and corruption of the government machinery, lead to a lack

of integration of ICT based systems into the core business processes of an organization and the long term financial sustainability aspect of ICT infrastructure is ignored.

b. Human Resource Aspects

There is a lack of institutionalized means of developing related skills. Government implementation projects suffer from lack of skilled human capital. Only ICT skill courses available for the civil servants. These are not enough to bridge the gap. There is no much facilities for the civil servants to enhance their 'soft-skills' associated with managing implementation of e-Governance systems. Government institutions may explore introducing courses on 'change management', etc. to address such deficiencies.

Incentive for acquiring ICT skill is essentially required. The lack of incentive is considered as one of the reason for lacking of ICT skilled human resources in the government. Indeed, in most government offices the use of IT is mostly self-motivated and a matter of individual self-development.

c. Economic Aspects

Like most developing countries, Bangladesh faces difficulties in investing large sums in e-governance system from its own budget. Absence of pro-private sector policies obstructs the potential source of private investment.

It is needed for building capacity of the civil servants to conduct cost-benefit and results-resources benefit analysis before approving e-governance projects. Managerial capability and technical know-how is an important factor to analyze the cost-benefit scenario and return on investments to assess financial sustainability of a project. It is an important reason for which the private sector remained as a skeptic bystander rather than a active partner in e-governance. As a result E-governance in Bangladesh could not meet the expectation of the people.

d. Social Aspects

Bangladesh is a country where disparities between haves and have-nots are ever increasing. Introducing ICT in the governance mechanism is facing the challenge of ensuring equitable access to e-governance services by all people of the society. It is essential to create public awareness with regard to e-Governance services that could be made available to everyone.

There are three social aspects that come under e-Governance challenges. These are

(1) Lack of literacy and a weak basic education standard,

(2) Standardization of Bangla for official use, and

(3) The 'Brain Drain' of ICT skilled human resources from the government.

e. Administrative Aspects

Senior government officials should come forward with regard to develop e-governance and the benefits inherent to it. The lack of awareness about e-governance systems, the senior management of government organizations remains inactive for its development. Such lacking of acceptability often means lack of sustainability of the system and even failure to implement such a system.

E-governance requires rethinking the standard operating procedure. The existing administrative rethinking mechanism is not aligned with e-governance activities and plans. Such lack of coordination between administrative reform and e-governance is another challenge.

In absence of central e-governance, coordinating and monitoring entity the tasks of prioritizing and controlling the quality of the e-governance projects remained as a challenge in Bangladesh.

f. Legal Aspects

The nation still needs to strive to have an operational regulatory / legal framework including relevant Cyber Laws. While the ICT Act has been approved recently, the work of drafting the bylaws (19 of them) and rules might take still some time.

g. Local Aspects

There is a dearth of local content available in the country. This plays an especially important role in the government since even if an officer is connected to Internet the relevant knowledge resources available to him is limited. This often limits the need or wants on the part of government staff to access the Internet as a part of their normal working routine.

5. National strategy of E-Governance

a. E-governance Awareness among public servants:

b. Facilitate public private partnership model to work:

c. Enhance access to ICT tools for citizens:

d. Creation of local content:

e. Adopt open standards and open source solutions:

f. Plan for the long term:

E-governance is a strategic choice. A nation needs to be sufficiently ready before implementing of e-governance objectives. A national e-strategy is required the following six fundamentals elements of e-governance readiness.

a. E-governance Awareness among public servants:

Training courses for government officials should move beyond the office productivity suite to conceptual courses that enable them to conceive ICT as a strategic asset rather than operational tools.

b. Facilitate public private partnership model to work:

E-governance initiatives are often capital intensive and have to compete with projects addressing other national development priorities. E-governance projects are often more risky than more traditional development projects. Most countries that are seriously pursuing E-Government have made partnership with the private sector to share the costs and risks of starting and running e-Government projects. A concrete policy framework and directive is needed to encourage the private sector of Bangladesh.

In this context, the government needs to look into the possibility of outsourcing most of the service delivery and substantial part of service production function to the private sector.

c. Enhance access to ICT tools for citizens:

The government needs to ensure equitable access to government services delivered online to all potential users. It is therefore important for the Government to invest resources and introduce policies to extend access to ICT throughout the country. Participation of public sector needs to be ensured to speed up infrastructure roll out. Innovative means of content delivery like mobile telephony, community radio, etc. based solution should be encouraged and explored.

d. Creation of local content:

The government should take the lead in creation of locally relevant content in the local language. Preservation of local knowledge in easily understandable forms must be encouraged. Most of Bangladeshi's cannot read and comprehend written text strategies. To encourage them, the voice and video data should be developed and implemented.

e. Adopt open standards and open source solutions:

Bangladesh can embark on a single project to develop both its hardware and software solutions and then proceed gradually. Bangladesh should undertake a small but manageable project and gradually build up its e-governance maturity. It is important that the nation adopts an open architecture for easy interoperability.

f. Plan for the long term:

E-governance systems bear fruits only in long term. Failure in experimental period often results an unnecessary frustration and experimentation resulting in the loss of resources and motivation among the users.

6. E-governance initiatives in Bangladesh:

a. Automation of Internal Processes:

b. Electronic Birth Registration:

c. Financial Management:

d. Government Forms Online:

e. Hajj Web Site:

f. MIS for Project Management and Transparency:

g. National Board of Revenue:

h. Personnel Database:

i. Railway Ticketing:

E-governance initiatives in Bangladesh are a few truly successful initiatives. Some of them are included here.

a. Automation of Internal Processes:

Bangladesh Bank began to computerize its functions. Most of the government offices started investing in automation. The Bank is only among the handfuls that have been successful in integrating ICT into the core business processes of the institute. Today it is one of the most fully computerized public institutions in the country. The current system actually automates most of the Banks operational processes and some of the most important strategic processes including monitoring of commercial bank transactions.

b. Electronic Birth Registration:

Electronic Birth Registration System was introduced by The Rajshahi City Corporation (RCC) and the Local Government

Division of the Ministry of Local Government with technical and financial support from UNICEF. This is probably the best local level e-governance example of Bangladesh. A local government body, in their own initiatives and leadership and with support form a development partner took such a bold step forward. The system also doubles as an immunization management system. Once registered, the system also generates an immunization schedule for every child. To system generated ID is also used to get admission in the public schools of the city.

c. Financial Management:

Two projects such as Reforms in the Budgeting and Expenditure Control (RIBEC-1 and RIBEC-2) became unsuccessful and RIBEC-2A and then RIBEC-2B became successful. Ministry of Finance has proceeded gradually and the ministry of Finance now has developed a quality MIS system. It is successfully used for budget planning, sensitivity analysis, impact analysis, financial projections and other core processes of the ministry.

d. Government Forms Online:

Accessing government forms online is made possible by the Prime Minster's Office of Bangladesh though a project funded by UNDP Bangladesh. This not only saves time but also the cost and hassles associated with the traveling to the government offices located at a distance.

e. Hajj Web Site:

The Ministry of Religious Affairs, GoB introduced the Hajj Web Site in 2002 to provide service for the pilgrims who go to Mecca to perform holy Hajj. During the Hajj, the website also acts as an important information portal for the family members of the pilgrims and other interested persons and organizations. One of the best examples of a Public-Private Partnership project, the site provides timely and reliable information to a large segment of the population.

f. MIS for Project Management and Transparency:

Department of Roads and Highways, Ministry of Communication, GoB, developed this MIS as a component of a World Bank funded project for the institutional development of RHD. The eGovernment initiative of RHD involved the launch of a website that provides a variety of information, data and notices to users. Website users include

the private sector, related government offices, ordinary citizens, and donor agencies.

g. National Board of Revenue:

Several development projects like Asian Development Bank funded 'Customs Administration Modernization Project', International Development Agency funded 'Excise, Taxes & Customs (ETAC) Data Computerization Project', World Bank funded 'Modernization and Automation Project' etc. much of the core processes of NBR and some of its citizen services has already been computerized and implemented successfully.

h. Personnel Database:

The Personnel Management system (more of a database with some analytical reporting) of the Ministry of Establishment is probably the oldest e-government initiative that is still is in use and in demand. The database in maintained by the technical personnel with in the ministry and maintains the personal information card for each government employ of the 'Administration' cadre including their respective annual confidential reports.

i. Railway Ticketing:

Technically, Railway ticketing might not be a simpler e-government project but from people's convenience perspective, this is one of the important one. Bangladesh Railway outsourced the job to a local IT vendor. With a few technical hiccups the system was put to operation in 1996. The vendor owned operated and maintained the system till early 2002. The system was than transferred to Bangladesh Railway, who later decided to outsource its operation to another private vendor.

j. Voter ID Card Preparation:

Under the supervision of the Care Taker Government of Bangladesh voter ID card preparation started In the year 12007 and ended in 2008. This is a massive programme completed with by using our own IT manpower. It is the commitment of the Care Taker Government to the public for a free and fair election. Election commission with the collaboration of Bangladesh Army successfully completed this massive program. This is am best example of E-governance of Bangladesh.

Chapter–24
E-Readiness
E-Readiness: Bangladesh Perspective

---

1. What Is E-Readiness

Readiness literally means the state of being ready or prepared for use or action, prompt willingness or a natural effortlessness to do something.

E-Readiness means Electronic Readiness. It is the degree of status to which a country is prepared to participate in the Computer Network World. It is a state of relative advancement in the areas of ICT adoption and the most important applications of ICTs.

The value to a country of assessing its Readiness lies in evaluating its unique opportunities and challenges. Most countries

will not be uniformly ready across all evaluation criteria. A country may be in well position for some applications of ICTs, but unable to use others. The scope and detail of the Guide's output makes it a powerful tool for identifying a community's strategic priorities for participating in the Networked World.

E-Readiness is the ability to use Information and Communication Technologies (ICT) to develop country's economy and to foster its welfare. There are several benchmarking indices at the macro level and those are calculated by the UNPAN, World Bank, EIU etc.

2. Definition of E-Readiness:

According to Harvard University

"E-readiness is the degree to which a community is prepared to participate in the Networked World. It is gauged by assessing a community's relative advancement in the areas that are most critical for ICT adoption and the most important applications of ICTs. When considered together in the context of a strategic planning dialogue, an assessment based on these elements provides a robust portrayal of a community's e-readiness. The value to a community of assessing its Readiness lies in evaluating its unique opportunities and challenges. Most communities will not be uniformly ready across all evaluation criteria. The result is not a simple yes or no, but rather a complex map or detailed snapshot of a community's potential. A community may be well poised for some applications of ICTs, but unable to use others. The scope and detail of the Guide's output makes it a powerful tool for identifying a community's strategic priorities for participating in the Networked World."

3. E-readiness - Work Areas

E-readiness has the following work areas:

a. Telecommunications , IT and Internet
b. Human Resources Development
c. Regulatory Framework
d. Public Institution
e. Corporate Sector

4. E-readiness is of five categories

1. Technology (Network Access): The availability, cost and quality of ICT networks, services and equipment.

2. Networked Education: The educational system integrate ICTs into its processes to improve learning. Technical training programs in the country that can train and prepare an ICT workforce.

3. Networked Society: Individuals are using Information and Communication Technologies at work and in their personal lives. There are significant opportunities available for those with ICT skills.

4. Networked Economy: Businesses and governments are using information and communication technologies to interact with the public and with each other.

5. Network Policy: The policy environment promotes or hinders the growth of ICT adoption and use.

5. E-readiness Principles

The following is a preliminary list of the fundamental principles of E-readiness. These should be respected and reinforced as much as possible. These may bring the great changes on national society and economy.

a. Democracy and Social Solidarity
b. Shared Economic Growth
c. Integral Development of Human Resources
d. Citizen Safety and Honesty

a. Democracy and Social Solidarity: Democratic society should continue to be promoted through ICTs. Citizen can participate in political electoral process and their decision-making. The incorporation of all social sectors in these processes is possible. It also reinforces individual rights and guarantees by improving access to information and faster on-line bureaucratic processes. Democratic society is the beneficiary and user of ICTs.

b. Shared Economic Growth: Economic growth is a desirable factor. The main objective of growth must not be to explicitly redistribute wealth by moving it from one chosen group to another. This would not promote the kind of free market regime that a society wishes to encourage. The goal of economic growth is to prepare the country to generate opportunities for business and investment. Both the smallest and the most powerful businessmen would be benefited by

the technological revolution. All the citizens can enjoy globalize economy and society by this process of insertion. From the point of view of economic development, growth must be such that its fruits are enjoyed by small and medium sized companies (SMEs) as well as by large companies, either national or transnational.

c. Integral Development of Human Resources: Education is a fundamental pillar of a society. The Knowledge Based Economy plays more critical role in the economic growth of the country. The globalization of world markets will determine what developing countries will produce and what they will import. Knowledge is the essential factor in new productive processes. Countries those are better equipped to cover this need will be the ones to position themselves as leaders in the new world. The educational system of any country will require adjustments to incorporate new skills in many areas of human knowledge.

d. Citizen Safety and Honesty: Citizen safety is another fundamental pillar in the democratic life. This can be achieved by social stability and maintenance of peace and justice in civil society. Economic growth, reduction of poverty levels and moral values of society can support citizen safety, promote honesty and altruism in general. Constant improvement of telecommunications infrastructure could be a useful means of obtaining these objectives.

6. E-readiness Methods

Methods for evaluating the e-readiness are as follows:

1. Identifications of the participants and of the ad-hoc working groups

2. Definition of Indicators. Each participant or working group will propose indicators that reflect e-readiness. Obviously, as the work and analysis of results advances, other indicators, both qualitative and quantitative, will arise for e-Readiness evaluation.

3. Identification of Information Sources. In this stage, each of the participants identifies the institution, documents, Internet sites that best provide the information necessary to evaluate e-Readiness. In the Telecommunication infrastructure area, for example, cooperation from institutions like BTTB or Mobile Phone companies is fundamental in achieving this objective.

4. Valuation/Assessment of Indicators. Valuation or estimation of the utility of indicators used for the evaluation of e-Readiness will be made after defining information sources and analyzing the information they produce.

7. E-readiness Strategy

The Readiness assessment is the starting point in a participatory planning dialogue. It should be intensify awareness of the opportunities and challenges of joining the Networked World.

A planning process should be taken as a true partnership among businessman, government and other members of the country. The process should encourage but not require participation from the whole community. Participants should be key stakeholders that might include local ISPs, high-tech companies, business users, appropriate government officials, educators, universities, bankers and community groups.

Just as the other components of Readiness have been assessed, the nature and progress of the planning dialogue that is currently underway within the community should also be carefully understood. This is valuable whether a plan has already been put into action or if there is not yet any planning underway.

8. E-readiness E-Policies

Several issues regarding E-readiness policies are outlined here; which are as follows:

1. There is a Telecommunication Act in Bangladesh.
2. The Ministry of Communication and Information

Technology is the Competent Authority in the Telecommunication field.

3. Law regarding the Electronic Signature should be enacted.

4. There should be a Government ordinance regarding Access to the Electronic Communications Networks and to the associated infrastructure.

5. The tax regime treats equally the Bangladeshi and the foreign investors. There are no special incentives for foreigners to invest in Bangladesh.

6. An office for investors should be established in order to reduce bureaucracy and corruption and to achieve transparency in the investments environment.

9. Legal Framework for E-readiness

1. Telecommunications Regulation
2. License granting
3. The authorization
4. Protection measures of the users

1. **Telecommunications Regulation :** Projection, installation, maintenance, interconnection ownership, of the communication equipment, as well as communication services supply or other activities relating to this field can be performed by any legal or natural person qualified with respect to the legal provisions applicable to this matter. The telecommunication services suppliers and the operators of the communication nets are obliged to respect the information confidentiality emitted, transmitted or received through their communication equipment.

2. License granting: The activities' performance by public operators and basic communication services providers may be developed on the basis of a license issued by the Competent Authority Considering that the market or the available radio electric spectrum is limiting the competition, the providers of other communication services may also operate on the basis of a license issued by the Competent Authority.

The beneficiary of such a license can be only a Bangladesh legal person. The license may be issued only for a certain type of net or for certain types of communication services as determined by the Competent Authority. The Ministry for Communication and Information Technology may impose territorial limitations for the license granted to a communication services supplier or to a public operator. The law permits the ownership of several licenses by the same legal person.

The Ministry for Communication and Information Technology may allot the license trough tender or direct allotment. It is also for the Ministry to determine the number and type of licenses. The decision regarding the procedure of allotment (tender or direct allotment) must be justified.

The legal provisions stipulate the requirement that the tender follows a transparent procedure. Thus, the tender has to be advertised in central and local media and the conditions to be fulfilled by the tender bidders must be explicitly specified by the Competent Authority.

The provisions of the license stipulate the rights and obligations of the owner. The licenses can be renewed in accordance to the legal provisions. The conditions stipulated in the license may be modified with the mutual consent of the Competent Authority and the licensee.

The license can be totally or partially, temporarily or finally withdrawn by the Competent Authority in case that the licensee does not respect its obligations or does not respect the legal provisions regarding the confidentiality and inviolability of the communications.

The withdrawal may be decided only after a prior notice addressed to the licensee, underlining the non fulfillment of the obligations. The licensee may reply to the notice within 30 days. Considering the answers, the competent authority must verify the real situation and decide whether to withdraw or maintain the license.

The licensees intending to enter any property in order to install or maintain the transmission wires or the terminal points must conclude a written agreement with the owner or possessor of the property. This agreement is necessary only for the initial connecting of the subscriber to the net of the licensee. Any appeal or litigation regarding this matter will be solved in accordance to Law prescribed.

By default of the owners or leasers consent, the communication works can be performed on the basis of a definitive and irrevocable judgment or, in case of emergency, on the basis of an injunction judgment. All judgments must be stated in accordance with the legal provisions that are granting the property right and the Law regarding the expropriation of property for a public purpose.

3. The authorization : The communication services suppliers that are subject to the free competition market and the independent operators are allowed to perform the communication activities on the basis of an approval issued by the Competent Authority. The beneficiary of the approval may be a natural or legal person.

The authorization will be issued in accordance to the procedure settled by the Competent Authority. The authorization will not be issued, if there are any evidences that the service or communications nets could harm the security or health of the users or the confidentiality of the communications or if there are no available frequencies.

The authorization is personally and must not be transferred. It will be issued for a term of 5 years, with the possibility of being renewed or

withdrawn after a prior 30 days term of grace, in which the owner has to undertake all the necessary steps in order to act legally.

4. Protection measures of the users : The Competent Authority approves the content of the agreements to be concluded between the license owners and the users. The competitors of the public operators and telecommunication services must not be treated differently. While requesting the access to the net or to the services provided by these ones, under the condition that the approval of their request is the basis for the development for other telecommunication services and there are no grounded reasons for preventing the access. In this situation, they should benefit from the same technical and financial conditions as for any other user.

Public operators and communication services suppliers that hold a dominant position on the communication market are obliged to respect "the open net clause." All conditions regarding the free access to the nets of the public operators and to the communication services are dedicated to the public as well as the efficient use of the services.

It is forbidden for the license owners to use the income achieved from the operation of the nets or services granted by the license in order to subsidize the tariffs for the activities subject to authorization or to free competition. The special legal provisions regarding the telecommunications must be applied in accordance to the Law. Any litigation between the operators and the Settlement Authority will be solved in accordance to the administrative contentious legislation.

10. E-Readiness : Bangladesh Perspective

Preparedness of a country on e-governance, e-learning, e-connectivity, e-commerce and e-policy and to assess the national need is essential. With this readiness a nation like Bangladesh can achieve a certain level of national standard for promoting sustainable development and poverty alleviation of Bangladesh.

Internet came late in Bangladesh. But the first main frame computer reaches the country in 1968 and the first PC in 1981. Starting with a few hundred PCs in the early years, the current.PC users' number may be satisfactory. It is a good sign for Bangladesh to utilize the blessings of ICTs for the development of the country and to increase the transparency of the Government machineries for the benefit of the citizens.

The e-readiness of a country depends on the following standard facilities:

a. Network Access and Internet Penetration availability,
b. Information Infrastructure development status,
c. Internet Affordable capacity of the citizen,
d. Quality Assurance Network structure availability,
e. Hardware and Software situation of the country
f. Service and Support provided by public and private sector,
g. Extended Education facility using ICT
h. Development and training of ICT Workforce
i. Individuals and Organizations of networked society,
j. Locally Relevant Contents availability,
k. Scope of ICT in Workplace
l. ICT Based Employment Opportunity
m. E-Government
n. IT Act
o. Telecommunications Regulation
p. ICT Policy

Implementation of information and communication technology is necessary for mass applications. A study on the ICT infrastructure development and e-readiness assessment has became the national importance for this country to be a important member of global networked world.

Primary target of an IT development initiative is relate to high speed data transfer and huge collaboration of infrastructure development. The mobile telephone in Bangladesh has developed tremendously. But due to non-availability of BTTB

land telephone to the rural community, it would be extremely difficult and expensive to extend any computer network to the grass root level of the country. Bangladesh entered into the optical fiber super highway. This is a one step ahead towards ICT development.

Bangladesh has taken and formulated an action plan at national level for contemplating the information and communications technology towards sustainable development by raising the e-knowledge of the general communities.

Internet is now widely available in all major cities of Bangladesh. Most of the Upazila brought under the internet networked. But the development of IT was delayed in Bangladesh. Due to lack of infrastructure and lack of knowledge; e- mail and Internet users, were unable to avail the hardware resources. So the IT revolution in the country is hampered.

The large unemployed youths who sought a new career in computers and got them enrolled in self-styled computer training facilities that opened the path to IT in Bangladesh. The professional groups moved in to offer training facilities, the better-educated students fresh from the university with the financial support of their parents took advantage of the improved environment. These youths are now emerged as the core group of IT professionals.

The government has taken a few praiseworthy critical decisions for promotion of ICT in the country. These are

1. Government has waived all taxes on all equipment related to IT;
2. Government has enacted a bill granting copyright to intellectual property; and
3. Government has taken necessary steps to build an IT village just outside the capital city.
4. Bangladesh IT Policy 2002 has enacted, and
5. Bangladesh IT Act has draped and on the way to pass as an Act.

The real contribution of the private sector has been in the area of HRD and the Bangladeshi and non-resident Bangladeshi (NRB) professionals have just begun to make their inroad into software development for the overseas clients.

Readiness is the degree to which a community is prepared to participate in the Networked World. Community's relative advancement in the areas is most critical for ICT adoption. Bangladesh, being an over populated country in this region and being at the trail among the countries with e-readiness and hence, adoption of generalized information technology at mass level of implementation is at a low end. For a strategic planning the exact areas of intervention, put emphasis on specified sectors and formulate policies for better implementation of ICT in the country is essential.

It would be appropriated to take an initiative for assessment of the present e-community in Bangladesh. The study should be able to reveal

the juncture of past and present environment through the assessment and also, be able to foresee the long term future by offering indication on formulation of strategic plan.

The Internet came late in Bangladesh, with UUCP e-mail beginning in 1993 and IP connectivity in 1996. Through different Internet Service Providers (ISP), who is offering Internet services with bandwidth ranging between 65Kbps and 2Mbps through VSAT, Broadband and Zacknet downlink. In June 1996, the government decided to allow private entrepreneurs to act as ISPs using VSATs (Very Small Aperture Terminal). The growing demand of the society and the congenial global atmosphere towards Internet has made the entrepreneurs to re-think their policies and strategies to accommodate the newly emerged rapidly enlarging target group.

Demand did not inclined high compared to the huge population base, because most of them live in rural areas where minimum tele-communication infrastructure is missing and at the same time purchasing power of the general communities limiting

Internet connectivity with prevailing socio-economic conditions. The Internet facility developed tremendously in mostly town areas. Initiate is to be taken to bring the rural areas within the internet Networked. Bangladesh has also taken due measure for the rural development through public and private sector.

Affordability of Internet in Bangladesh largely depends on the basic telecommunications infrastructure. As mentioned earlier that the country has a very low telephone density as compared to other countries in this region. Apart from this service Grameen Phone is providing WAP facility through their cell phone to its customers.

Private sector ISPs are playing a major role in popularizing and enhancing Internet backbone of the country.

The number of Internet subscribers is increasing rapidly. At recent times, there has not been any established statistics regarding the characteristics of the users. But, it has revealed that most of the clients are from student community and youth group of Bangladesh.

IT facility and computerization of schools in Bangladesh is also an important factor. But it is very difficult to develop the standard of the schools to a certain level for several barriers. To understand the training needs in ICT, access to the ICT, facility of E-learning among

the rural student community, the need of improvement in syllabuses, need for trainers and teachers at grass root level is essential to enhance the quality of our rural people.

In order to develop a national sound telecommunication infrastructure to support the economy and welfare of the country by providing telecommunication facilities on demand, assuring satisfactory quality of service and ensuring value to the customers, a sound National Telecommunication Policy is essential. The strategic vision of the government is to facilitate Universal Telephone Service throughout the country and where there is a demand, all those value added services such as cellular mobile telephone paging, data service, access to Internet, voice mail and video conferencing- all at an affordable cost. Bangladesh is developing toward that goal and enacted National Telecommunication Policy, 1998.

Bangladesh government has taken liberal IT policies to enhance the mass awareness on information technology. Complete withdrawal of tax on computer and computer related items has created extra enthusiasm among general society through increased participation in computer based activities including training and software development.

The National Telecommunication Act, 2000 autonomous regulatory commission, the Bangladesh Telecommunication Regulatory Commission (BTRC) has been formed, for adapting the fast changing technologies in the telecommunications sector and supervises the services to ensure that the interest of the users is protected. Formation of National Telecom Regulatory Commission (NTRC) is another step for the development of ICT.

With a view to reducing pressure on its fixed lines and facilitating operations for the Internet Service Providers (ISPs), the

BTTB introduced the European Standard-1 (E1) system. The E1 line will be able to ensure better bandwidth. The optical fiber super highway will tremendously changed the performance of the ISPs and other ICT sectors.

A society has been formed with leading private entrepreneurs engaged in promoting computer products in Bangladesh and it is providing assistance in designing and implementing policy issues and related affairs at the rudimentary stage of the country. Bangladesh Computer Samity is playing a vital role in this field. ICT has become

part and parcel of every day's life and the indicators needed to measure this effect need more in-depth enumeration and analysis.

The evolution of the digital economy and the explosion of e-commerce have created new challenges for entrepreneurs who provide data based solutions to today's businesses. The emergence of the WWW as a dominant force in business has contributed to a dramatic increase in the amount of data available to organization. These trends have heightened reliance on traditional database applications and increased the demands on these applications in terms of both performance and reliability. In addition, the changes in the way of doing business have created demand for new features that exténd database applications beyond the traditional feature set and prepare them to do service in the new economy.

In contrast to the global situation, the Bangladesh Government has also been found promoting the use of electronic transactions and is committed to creating an environment in which these transactions will be completely secure. Though this process is at a very rudimentary stage, but a few of the renowned organizations are working to prepare a policy guideline for the country.

In this respect, a certification authority for issuance and management of digital certificates that are needed to secure electronic transactions is being formed. Use of international credit cards like VISA, MasterCard etc. is increasing rapidly and is being encouraged. Along with these measures, necessary legal framework, so that the guiding principles, rules and legislation for e-commerce are in place, is in the process of formation. Background analysis and further information will be provided regarding ICT based HRD and employment opportunity in the final submission. Bangladesh already on the way to formulate the legal frame works. IT policy has been formed. IT Act is drafted and on the way to approval.

In a unique collaboration between the garments and IT sectors, BGMEA, DataSoft, Bangladesh and eVastra, USA have created www.bangladeshgarments.info - the country's first Business-to-Business (B2B) web portal. It functions as a virtual global marketplace where the country's factories are united, thus presenting a significant presence to draw buyers from around the world. With this user-friendly and fully functional site, Bangladesh's garment exporters have been put on the e- Commerce fast-track. The www.bangladeshgarments.info site

has been created for the BGMEA members with all the features required by Bangladesh's garments exporters in mind.

Bangladesh Government has taken several initiatives in this respect. USAID, UNDP and a few other agencies are conducting case studies. Data and information will be accommodated in the updated reports as per the availability.

In Bangladesh, the IT has been declared as the most thrust sector and the Government and the private sector have committed themselves to collaborate actively "with a view to improve the quality of life of its people and acquire the necessary capability to meet the challenge of rapidly growing demands of the information age". It is believed that the IT will create opportunities for all citizens, including the disadvantaged and those living in remote areas. The government is committed to setting up appropriates IT organizational and institutional structures, taking measures to strengthen HRD and educate leaders, both in the public and private sectors, on the appropriate use and benefits of IT in nation building.

The government sees itself responsible for creating a "regulatory environment that facilitates the rapid growth of all networks, promoting interoperability, data security and protection of intellectual property rights". The country expects rapid growth rate in IT spending, preferably with the state support, to reach a target of at least 25% growth per annum. Major investments, preferably in collaboration with foreign firms, are being encouraged towards creating "a world-class industry and IT professional services sector".

The high-speed fiber optics communication channel of Bangladesh Railway could be used for setting up of a national data communication network for nationwide transmission of data. Plans for setting up IT village, software technology parks (STPs) with satellite data communication facilities especially for software development/export companies, and introduce need-based R&D activities in universities, BITs, Colleges, Polytechnics by the Ministry of Information Technology have encouraged expatriate Bangladeshi's to undertake substantive investments. A national software development plan (NSDP) to develop domestic software market is already underway.

Development of National Data Resource Centre Network (NDRCN), a network of MIS of different ministries, localities and

sectors including education, health, agriculture, industry and natural resources, environment and ecology is underway.

The advent of information technology is growing stage. Particularly, many of the necessary institutional, legal and physical infrastructures necessary for its further development are being laid down. Making of IT is a preferred medium for people exchange of information and interaction and in the process makes other related endeavors economically and socially beneficial to Bangladesh.

The information infrastructure, comprising all information related institutional bodies, networks, databases, broadband communication and broadcasting systems, is the backbone of the modern information age. Without adequate information infrastructure a country will be unable to reap the rewards of the information age and will be excluded from the global information superhighway and the cyberspace.

ICT is a fast growing technology and many developed countries already reached to a commendable position in this aspect. Even, recently a large number of developing nations made unprecedented progress. To follow the technological trend and the level of expertise of these countries and attain a sustainable growth in this sector and to compete in the expanding global IT market, a separate IT ministry was the demand of the time. Fortunately it has been formed and all out effort from this newly established ministry is extremely essential for ICT related policy initiations in Bangladesh.

The whole country should be brought under telecommunications network at the earliest possible time and all existing analogue channels should be readily converted to digital, covering the whole country under PSTN. The BTTB can create facilities for low-cost high speed communication link and set up ISDN/HDSN lines throughout the country. Especially it is required to introduce high bandwidth T1 and E1 lines and high speed data transmission channels. Telecomm facilities should be specially focused to rural and remote regions following the usage pattern, but not compromising the quality of service and justification of cost. The time has come to privatize the Telecomm sector.

Emphasis should be given to extend information infrastructure, awareness development, human resource development, and distribution of resources. Policy guideline should be prepared for promotion of e-commerce and e-governance. In this way Bangladesh will become healthy ICT user.

ABBREVIATIONS

ADAB – Association of Development Agencies in Bangladesh
BARC – Bangladesh Agriculture Research Council
BBS – Bangladesh Bureau of Statistics
BELA – Bangladesh Environmental Lawyers Association
BIDS – Bangladesh Institute of Development Studies
BOU – Bangladesh Open University
BUET – Bangladesh University of Engineering and Technology
BUP – Bangladesh Unnayan Porishad
DCCI – Dhaka Chamber of Commerce & Industries
DLRS – Department of Land Records & Survey
DOE – Department of Environment
DPHE – Department of Public Health & Engineering
EGIS – Environment & Geographical Information System
FEJB – Forum of Environmental Journalists of Bangladesh
FTP – File Transfer Protocol
IEB – Institute of Engineers in Bangladesh
IUCN – International Union for Conservation
LAN – Local Area Network
LGED – Local Government Engineering Department
PMU – Project Monitoring Unit of SEMP, MoEF
SDNP – Sustainable Development Networking Programme
SEMP – Sustainable Environment Management Program
SWMC – Surface Water Modeling Center
UGC – University Grants Commission
US – Unnayan Shamunnay
VSAT – Very Small Aperture Terminal
WAN – Wide Area Network

CHAPTER - 25

E-learning

1. What is E-learning

E-learning means Electronic learning. It is a term used for computer-enhanced learning by using Information and Communication Technology (ICT). It is a new concept and method for education of all level.

E-learning is naturally suited to distance learning and flexible learning. It can also be used in conjunction with face-to-face teaching. In this case the term Blended learning is commonly used. E-Learning can offer learning scenarios, worksheets and interactive exercises for children. The term can also be used extensively in the business sector On-line training.

In higher education a Virtual Learning Environment (VLE) is to be created. It may be the combination of Management Information System (MIS) and Managed Learning Environment. A growing number of physical universities and On-line colleges have begun to offer a select set of academic degree. The courses can be delivered completely through On-line. Several universities offer online student support services. These are On-line advising, registration, e-counseling, On-line textbook purchase, student governments and student newspapers.

Modern technologies and computers network has changed methods of education and training. This new idea of education is e-learning programs. The technology-based training and education is e-learning which changed the mode of human resource development. Various terms are used for these emerging training methods. These are-

1. Asynchronous learning,
2. Distributed learning,
3. Online learning,
4. Web-based learning,
5. Computer-based training,
6. E-learning and
7. Distance learning

E-Learning would be evolved to systems consisting of a variety of channels and technologies. It can take the form of courses as well as modules and smaller learning objects. It may incorporate synchronous or asynchronous access. It is distributed without geographical limits.

Three major factors of e-learning program are as follows :

1. Cost efficiency,
2. Learner satisfaction and
3. Learning resources.

2. History of E-learning

The PLATO System developed at the University of Illinois at Urbana-Champaign is the first general-purpose system for computer-assisted e-learning. The Plato system evolved with the involvement of Control Data. The first authoring software was used to create learning content. The authoring software was called Plato. The first CAI system of Math for K-6 had been written by The Science Research Council. Wicat Systems then created WISE as their authoring tool using Pascal and developed English and Math curriculum for K-6.

Using the Wicat system, the first complete CAI classroom for K-6 students was set up at the Waterford Elementary School. The first public CAI classroom with its own layout and design was implemented with the Wicat System by Baal Systems (later known as Virtual Systems) in Singapore as a joint operation between Wicat and Baal. From this design, all the computer learning centers were globally evolved and become the forerunners of eLearning.

3. Growth of E-learning

The pioneer of On-line learning institutions in the mid-1980s were the followings:

1. The Western Behavioural Sciences Institute,
2. The New York Institute of Technology,
3. The Electronic Information Exchange System - EIES,
4. The New Jersey Institute of Technology, and
5. The Connected Education.

Independent Student Media an organization that has developed a working curriculum. They instructs students through an Interactive On-line Textbook. The term e-Learning itself originated in the corporate literature of CBT Systems. Now millions of students are participating in On-line learning at institutions of higher education. All public higher education institutions, as well as a vast majority of private, for-profit institutions, now offer On-line classes. Digital native a new concept has become popular and there are generational influences on the future of e-learning.

4. E-larning Market

E-learning is considered as a worldwide industry in education sector. E-learning products are produced within the common market. Developments in Internet and multimedia technologies are the basic enabler of e-learning. There are three key sectors of the e-learning industry; these are

1. Contents of E-learning,
2. Technologies used and
3. Services provided.

There are two additional sectors, those are

a. Consulting sectors, and
b. Support sectors.

There are many organisations in E-learning market. These are-

a. SkillSoft,
b. Epic,
c. LearnKey,
d. Semanoor,
e. BlueU, and
f. LearningSteps.com

These are the leading innovators in the design and development of e-learning in the commercial world. SkillSoft is the largest company in the global market since 2006 and Epic is one of the largest e-learning content providers.

5. Technology of E-learning

Many technologies are used in E-Learning. These are as follows:

a. screencasts
b. ePortfolios
c. EPSS (electronic performance support system)
d. Palm pilots
e. MP3 Players
f. the use of web-based teaching materials
g. hypermedia in general
h. multimedia CD-ROMs
i. web sites and web 2.0 communities
j. discussion boards
k. collaborative software
l. e -mail
m. blogs
n. wiki
o. text chat
p. computer aided assessment
q. educational animation
r. simulations

s. games
t. learning management software
u. electronic voting systems

Most e-Learning situations use combination of the above techniques. The term Learning technology and Educational Technology, is generally used for technology in learning. It is much broader sense than the computer-based training or Computer Aided Instruction. It is also broader than the terms On-line Learning or Online Education which generally refer to purely web-based learning. In cases where mobile technologies are used, the term M-learning has become more common.

6. Advantages and Disadvantages of E-Learning

Advantages: The followings are the advantages of E-learning:

1. Flexibility,
2. Convenience, Ability to work at any place where an internet connection is available,
3. At one's own pace.
4. E-classes allow learners to participate and complete coursework in accordance with their daily commitments. This makes an e-learning education a viable option for those that have other commitments such as family or work or cannot participate easily. There are also transportation cost and time benefits.
5. Ability to communicate with fellow classmates independent of metrical distance,
6. Adaptability to learners needs more variety in learning experience with the use of multimedia and the non-verbal presentation of teaching material.
7. Streamed video recorded lectures and MP3 files provide visual and audio learning that can be reviewed as often as needed.
8. E-learning has considerable benefits when compared with organizing classroom training.

Disadvantages: The followings are the disadvantages of e-learning:

1. E-learning includes the lack of face-to-face interaction with a teacher.
2. Critics of e-learning argue that the process is no longer educational in the highest philosophical sense. Supporters of E-learning claim that this criticism is largely unfounded, as human interactions can readily be encouraged through audio or video-based web-conferencing programs.
3. The feeling of isolation experienced by distance learning students is also often cited, although discussion forums and other computer-based communication can in fact help ameliorate this and in

particular can often encourage students to meet face-to-face, although meeting face-to-face is often not possible due to the disarray of student's physical locality. Discussion groups can also be formed On-line. Human interaction, faculty-to-student as well as student-to-student, should be encouraged in any form.

7. Services of E-learning

E-learning services have evolved since computers were first used in education. There is a trend to move toward blended learning services, where computer-based activities are integrated with practical or classroom-based situations.

8. Free E-learning software platforms

a. ATutor
b. Bodington
c. Dokeos
d. KEWL
e. LRN
f. LON-CAPA
g. Moodle
h. Sakai Project

9. Non-free E-learning software platforms

a. Angel
b. Authorware
c. Blackboard
d. Brihaspati
e. Desire2Learn
g. Edumate
h. FirstClass
i. Knowledge Forum
j. SimplyDigi.Com Inc
k. Scholar360
l. WebCT
m. Litmos

10. What is open and distance learning

Open and distance learning is defined by the Commonwealth of Learning as, Distance learning is "a way of providing learning

opportunities that is characterized by the separation of teacher and learner in time or place, or both time and place; learning that is certified in some way by an institution or agency; the use of a variety of media, including print and electronic; two-way communications that allow learners and tutors to interact; the possibility of occasional face-to-face meetings; and a specialized division of labour in the production and delivery of courses."

11. What is learner-centered environment

The National Research Council of the U.S.A. defines learner-centered environments as those that, "pay careful attention to the knowledge, skills, attitudes, and beliefs that learners bring with them to the classroom."

The impetus for learner-centeredness derives from a theory of learning called constructivism. This views learning as a process in which individuals "construct" meaning based on prior knowledge and experience. Experience enables individuals to build mental models or schemas. This in turn provide meaning and organization to subsequent experience. Thus knowledge is not "out there", independent of the learner. The learner passively receives knowledge is created an active process in which the learner transforms information, constructs hypothesis, and makes decisions using his/her mental models. A form of constructivism called social constructivism. This emphasizes the role of the teacher, parents, peers and other community members in helping learners to master concepts. For social constructivists, learning must be active, contextual and social. In group setting, the teacher are facilitator or guide.

12. Uses of ICTs in E-education

Education policy makers and planners first of all should be clear about the educational outcomes that are being targeted. These broad goals should guide the choice of technologies to be used.

The potential of each technology varies according to it's is use. Haddad and Draxler identify five levels of technology are to be used in E-education. These levels are

1. Presentation,
2. Demonstration,
3. Drill and practice,
4. Interaction, and

5. Collaboration.

The following different ICTs are used in E-education.

a. Print,

b. Audio & video cassettes,

c. Radio and TV broadcasts,

d. Computers and

e. The Internet

These ICTs are used for presentation and demonstration. Drill and practice may be performed by using the whole range of technologies. Networked computers and the Internet are the ICTs that enable interactive and collaborative learning.

13. Use of Radio and TV in E-education

Radio and television broadcasting have been used widely as educational tools since the 1920s and the 1950s, respectively. There are three general approaches to the use of radio and TV broadcasting in education. The are

1. Direct class teaching, where broadcast programming substitutes for teachers on a temporary basis;

2. School broadcasting, where broadcast programming provides complementary teaching and learning resources not otherwise available; and

3. General educational programming over community, national and international stations which provide general and informal educational opportunities.

14. What is Teleconferencing and its educational uses

Teleconferencing refers to interactive electronic communication among people located at two or more different places. Teleconferencing is used in both formal and non-formal learning contexts to facilitate teacher-learner and learner-learner discussions, as well as to access experts and other resource persons remotely. In open and distance learning, teleconferencing is a useful tool for providing direct instruction and learner support, minimizing learner isolation.

There are four types of teleconferencing based on the nature and extent of interactivity and the sophistication of the technology:

1. Audio conferencing; Audio conferencing is the live exchange of voice messages over a telephone network.

2. Audio-graphic conferencing,: When low-bandwidth text and still images such as graphs, diagrams or pictures can also be exchanged along with voice messages, then this type of conferencing is called audio graphic. Non-moving visuals are added using a computer keyboard or by drawing/writing on a graphics tablet or whiteboard.

3. Videoconferencing; Videoconferencing allows the exchange not just of voice and graphics but also of moving images. Videoconferencing technology does not use telephone lines. This Videoconferencing uses satellite link or television network.

4. Web-based conferencing: Web-based conferencing, as the name implies, involves the transmission of text, and graphic, audio and visual media via the Internet. It requires the use of a computer with a browser.

15. What is the Use of computers and Internet for teaching and learning

There are three instructional use of computers and the Internet, namely:

1. Learning about computers and the Internet, in which technological literacy is the end goal;

2. Learning with computers and the Internet, in which the technology facilitates learning across the curriculum; and

3. Learning through computers and the Internet, integrating technological skills development with curriculum applications.

16. What is learning about computers and the Internet?

Learning about computers and the Internet focuses on developing technological literacy. It typically includes:

1. Fundamentals: basic terms, concepts and operations

2. Use of the keyboard and mouse

3. Use of productivity tools such as word processing, spreadsheets, data base and graphics programs

4. Use of research and collaboration tools such as search engines and email.

5. Basic skills in using programming and authoring applications such as Logo or Hyper Studio.

6. Developing an awareness of the social impact of technological change.

17. What is learning with computers and the Internet

Learning with the technology means focusing on how the technology can be the means to learning ends across the curriculum. It includes:

1. Presentation, demonstration, and the manipulation of data using productivity tools

2. Use of curriculum-specific applications types such as educational games, drill and practice, simulations, tutorials, virtual laboratories, visualizations and graphical representations of abstract concepts, musical composition, and expert systems

3. Use of information and resources on CD-ROM or online such as encyclopedia, interactive maps and atlases, electronic journals and other references.

4. Technological literacy is required for learning with technologies to be possible, implying a two-step process in which students learn about the technologies before they can actually use them to learn. However, there have been attempts to integrate the two approaches.

18. What is learning through computers and Internet:

Learning through computers and the Internet combines learning about them with learning with them. It involves learning the technological skills "just-in-time" or when the learner needs to learn them as he or she engages in a curriculum-related activity. For example, secondary school students who must present a report on the impact on their community of an increase in the price of oil for an Economics class may start doing research online, using spreadsheet and database programs to help organize and analyze the data they have collected, as well using a word processing application to prepare their written report.

19. What is telecollaboration

On-line learning involving students logging in to formal courses online is perhaps the most commonly thought of application of the Internet in education. However, it is by no means the only application. Web-based collaboration tools, such as email, listservs, message boards, real-time chat, and Web-based conferencing, connect learners to other learners, teachers, educators, scholars and researchers, scientists and artists, industry leaders and politicians—in short, to any individual with access to the Internet who can enrich the learning process.

The organized use of Web resources and collaboration tools for curriculum appropriate purposes is called telecollaboration. Judi Harris defines telecollaboration as an educational endeavor that involves people in different locations using Internet tools and resources to work together. Much educational telecollaboration is curriculum-based, teacher-designed, and teacher-coordinated. Most use e-mail to help

participants communicate with each other. Many telecollaborative activities and projects have Web sites to support them.

The best telecollaborative projects are those that are fully integrated into the curriculum and not just extra-curricular activities, those in which technology use enables activities that would not have been possible without it, and those that empower students to become active, collaborative, creative, integrative, and evaluative learners .There are currently hundreds of telecollaborative projects being implemented worldwide and many more that have either been completed or are in development.

20. Equity of access to ICTs in education:

There are wide disparities in access to ICTs between rich and poor countries, also between different groups within countries. The use of ICTs in education, existing divisions will be drawn wider along economic, social, cultural, geographic, and gender lines. Though every body wishes equal participation. The introduction of ICTs in education without careful deliberation can result in the further marginalization among the underserved and disadvantaged citizen.

For example, women have less access to ICTs and fewer opportunities for ICT-related training compared to men because of illiteracy, lack of education, lack of time, lack of mobility, and poverty. Boys are more likely than girls to have access to computers in school and at home. Not surprisingly, boys tend to enjoy working with computers more than girls. This is the situation of Equity of access to ICTs in education.

21. E-learning: Bangladesh Perspective

Nowadays it is expected that E-Learning may be an emergent system of learning. Development of computers and Internet technology are providing the necessary momentum for the E-Leaning systems. It is the demand of the time that this system of education should be introduced in Bangladesh. A practical and suitable framework is essential for this purpose.

A. Dimensions of E-learning: Bangladesh Perspective

In the context of Bangladesh the technological and resource support dimensions are rather crucial than all the others for establishing a successful E-Learning environment. The current ICT infrastructure of Bangladesh to E-Learning readiness is to be examined.

To create well designed, learner-centered, interactive, affordable, efficient, flexible, meaningful, distributed and facilitated E-Learning

environments various dimensions need to be explored. For establishing successful E-Learning systems, it should address all the issues involving the various dimensions of the e-learning environment. For successful E-Learning environments the following dimensions are required.

1. Institutional: The institutional dimension is concerned with issues of administrative affairs, academic affairs and student services related to E-Learning

2. Pedagogical: The pedagogical dimension refers to issues of teaching and learning concerning goals and objectives, content, design approach, organization, methods and strategies, and medium of e-learning environments.

3. Technological: The technological dimension of the framework examines issues of technology infrastructure in e-learning environments. This includes infrastructure planning, hardware and software related issues.

4. Interface design: The interface design refers to the overall look and feel of e-learning programs.

5. Evaluation: The evaluation for E-Learning examines both the assessment of learners and evaluation of the instruction and learning environment.

6. Management: The management refers to the maintenance of learning environment and distribution of information.

7. Resource support: The resource support dimension of the framework examines the online support and resources required to foster meaningful learning environments.

8. Ethical: The ethical considerations relate to social and cultural diversity, geographical diversity, learner diversity, information accessibility, etiquette, and the legal issues.

B. ICT Infrastructures in Bangladesh

1. Telecommunication Infrastructure:

Telecommunication sector in Bangladesh has been experiencing a huge boom in the last few years. Several private and public telecommunication operators have established their network all over the country. As they are expanding their operation to the most rural areas, they are also dwelling to improve the network performance and inclined to introduce latest technologies to the people. The recent growth of the telephone subscribers in Bangladesh is remarkable and in near future it will expand more rapidly.

2. Internet Infrastructure:

Internet use in Bangladesh has started since 1993 by providing offline email services. But Internet services to the public were not open until 1996. The first organization to get license as an ISP (Internet Service Provider) was Information Services Network (ISN - www.bangla.net). They set up a VSAT on June 1996 and installed necessary machineries including the Internet Server. They offered Internet services to the public through a dial-up network. It was the beginning of a revolution in Bangladesh towards the digital age of twenty first century.

The public sector operator BTTB took Internet to the rural-semi urban areas of Bangladesh. Starting from Dhaka they have provided dial-up ISP services to all the 64 districts of Bangladesh. BTTB also have some facilities in some Upazillas. It is promised that BTTB will connect all the 484 Upazillas of the country very soon. BTTB is using their countywide landline telephone exchanges to spread the Internet all over the country. Currently they have their DDN (Digital Data Network) exchanges at Dhaka, Chittagong, Rajshahi, Khulna, Barisal, Bogra, Comilla, and Jessore, Rangpur and Gazipur and distributing bandwidth using DDN services too.

Currently ISPs are using only VSATs to connect with the rest of the world. Some private organizations have also got their own VSATs, while the rest get leased lines from the VSAT owners and provide Internet services. Cost of accessing the Internet in Bangladesh is very high as compared to the average income of the people. Development of the software industry has suffered a lot due to the heavy charges of Internet and the slower data rate. ISPs are not capable of reducing the charges due to the higher cost of bandwidth. Having the submarine cable connection is supposed to solve the problem.

Mobile Internet has also been setup in Bangladesh. Grameen Phone, the largest mobile phone operator has already introduced WAP services. BDCom a local ISP has got WAP Internet services. WAP has not been popular as the charges are very high compared to the landline. Above all SMS and MMS are more popular to the mobile users.

3. Internet infrastructures for the rural people:

It is the reality that none of the 87,500 villages of Bangladesh got any kind of Internet connection so far. Even E-mail (offline or online) services are not available. Private sector companies are reluctant to go

to even the semi-urban areas due to the lack of economic viability. Public sector operator BTTB is looking mostly at the district towns. They are proceeding to go to the Upazila. Ministry of Science and ICT have two plans which can improve the overall situation. This are-

a. A plan to connect all the Secondary Schools to the Internet, which might take Internet to the villages, as most of the Secondary Schools are located in the rural areas.

b. Governments plan to connect all Ministries, Districts and Upazila is another project, which is also in the early stage of planning. This project is supposed to take Internet services to the villages.

Some specific obstacles to extend ICT to rural areas are as follows:

a. Electricity is yet to be provided to the most of the villages.

b. Although some of the semi-urban places like districts and Upazila have access to the Inter net, most of the people in the majority of the areas are yet to be connected.

c. The poor people in the rural areas are not literate to use an all-English based ICT system.

d. Internet is very expensive. Most people of the rural areas cannot afford to have a computer and Internet due to the high price.

4. Optical fiber link: ICT superhighway

Bangladesh has already connected to the global information superhighway through SEA-ME-WE-4 (SMW4) submarine cable. On this basis it is expected that the nationwide Internet backbone will be established and it is a matter of time.

SMW4's main specificity is flexibility. Up to 20 million voice calls or 60,000 broadcast television channels at the same time can be accommodated. The modern DWDM technology is capable to transport 64 wavelengths at 10 Gbps. Full-circuit routing, whether the operator owns a license in the destination country or not, is going to be the key feature of SMW4. An equipped capacity of 160 Gbps that will be upgradeable up to 1.2 Tbps, which guarantees enough capacity to meet the needs of Middle East, India, and other key destinations for the next decade. The project is going to support telephone, Internet, multimedia and various broadband data applications. The 14 countries linked are Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi Arabia, Egypt, Algeria, Tunisia, Italy and France with an extra landing station in Chennai, India.

The 28 KM connecting loop cable line from Cox's Bazar to the deep sea was also being laid. It is expected that the proposed submarine cable line network will increase the access capability of Internet in Bangladesh. It is also expected that with the commissioning of this cable line, the cost of bandwidth will come down dramatically. The submarine cable line will go by the pass of Cox's Bazar of Bangladesh. It will be 22000 Kilometer long and the landing station of Bangladesh will be at Cox's Bazar. Cost of the total project for Bangladesh is estimated to be Tk 3000 million.

The Turkish company Hesfible is assigned the job of installing fiber-optic network from Cox's Bazar to Chittagong. They will establish the network from the base station-Cox's Bazar to the port city of Chittagong. The cost of the 171-kilometer networking is estimated at Tk 28.41 crore. Under this scheme the company will also upgrade the 260-kilometer Chittagong-Dhaka optical fiber link.

The private cellular phone operators are currently utilizing nationwide 1800-kilometer long optical fiber network under Bangladesh Railway. Bangladesh Telegraph and Telephone Board (BTTB) have already established optical fiber link in most cities. The nationwide optical fiber backbone connected with the SMW4 submarine cable is the first step towards the next generation network in Bangladesh.

C. Problems of E-learning in Bangladesh:

It is very difficult for Bangladesh to utilize various facilities and opportunities provided by the modern E-Learning environments. Bangladesh has to face various problems. These are summarized as follows:

1. High percentage of illiteracy.
2. Low computer penetration.
3. Low Telephone density
4. Lack of continuous and uninterrupted supply of electricity
5. Old and outdated technology
6. Poor economic condition
7. Absence of legal infrastructure
8. Weak data communication infrastructure
9. Lack of public awareness about ICT
10. Lack of adequate human resources.
11. Brain Drain

D. Prospects of E-learning in Bangladesh:

1. E-Learning provides the opportunity to access the most up to date information and / or technology worldwide which are not possible to achieve through traditional system.
2. Human Resource Development will grow up to the global mark.
3. Students' interest in global education has increased in last few years. Many students go abroad to take international standard education in various fields. So students will be benefited from E-learning environments.
4. Bangladesh is approaching towards a remarkable position in computer utilization in various fields.
5. Sub-marine Optical Fiber network will provide necessary bandwidth in affordable cost to access E-Learning resources.
6. Increased opportunity in getting Global jobs.

E. Suitable Framework in Bangladesh

Most of the people of the Bangladesh have limited Internet access. To provide them with adequate online facilities, computer and Internet centers may be established. These Internet kiosks (cyber cafés) can serve as the 'community Internet access center'. These centers can be used as the E-Learning center. It is essential to spread the facilities among the people nationwide.

Distance learning program conducted by Bangladesh Open University (BOU), whose target is to spread education nationwide, by establishing their centers at schools in each

Upazilla. Village peoples are getting education from this successful program. This framework can closely follow the framework of E-Learning.

Considering all the factors it is mostly expected that spread of E-Leaning throughout Bangladesh is possible. E-Leaning framework which are prevailing and approaching that can take the effective role in enhancing the current education system in Bangladesh. Organizations from both public and private sectors including NGOs should take the necessary initiative for developing the systems as early as possible to get the benefits of E-learning.

CHAPTER - 26
E-journal

1. What is an E-journal

According to Chamber's Dictionary "Journal literally means a daily register, or diary: a book containing a record of each day's transaction: a newspaper published daily (or otherwise): a magazine: the transactions of any society".

The term E-Journal denotes Electronic Journal. E-Journal broadly may be defined as "any journal, magazine, e'zine, webzine, e-journal, newsletter which is available over the Internet."

E-journals are electronic versions of paper journals, periodicals or serials or any other publication. Every volume or publication of the journal can be viewed online as per limitation of the website. Individual articles or books are normally available on the website as PDF form. Some of the journals the library subscribes to will be available both in print and electronic form. Others E-journals will be available online. Electronic journals also called scholarly journals or magazines. It can be accessed via electronic transmission.

Scholarly journals are a specialized form of electronic document. The E-journals have the purpose of providing material for academic research and study. These are formatted approximately like printed journal articles. The

metadata is entered into specialized databases, such as DOAJ or OACI as well as the databases. For the discipline, these are predominantly available through academic libraries and special libraries.

Electronic journals are different type. This are-

1. Online journals;
2. Online versions of printed journals, and
3. These are consisting of the online equivalent of a printed journal, but with additional online material.

Most commercial sites are subscription-based. They also allow pay-per-view access. Many universities subscribe to electronic journals to provide access to their students and faculty. Individuals can also subscribe. There are open access journals available. They are increasing in number. The open access journal requires no subscription. Most working paper archives and articles on personal homepages are free. The collections in Institutional repositories and Subject repositories are also open access journals.

Electronic journals are generally published both in HTML and PDF formats. Some are published in any one of the two. Some early electronic journals were first published in ASCII text. Academic publishing describes the subfield of publishing which distributes academic research and scholarship. Most academic work is published in journal article or book form. Most of the academic publishing relies on some form of peer review or editorial refereeing to qualify texts for publication.

Established academic disciplines generally have their own journals and other outlets for publication. Many academic journals are interdisciplinary. They publish work from several distinct fields or subfields. The kinds of publications that are accepted as contributions of knowledge or research vary greatly between fields, as do review and publication processes. STM publishing is a frequently-used abbreviation for academic publications in science, technology, and medicine.

Business models are different in the electronic environment. Since the early 1990s, licensing of electronic resources, particularly journals, has been very common. Scholarly journals, is open access. There are two main forms of open access:

1. Open access publishing, in which the articles or the whole journal is freely available from the time of publication; and
2. Self-archiving, where the author makes a copy of their own work freely available on the web.

2. Definition of E-journal:

University of Leeds focus on the wide-ranging definition offered by the Colorado Alliance of Research Libraries;

"Electronic serials may be defined very broadly as any journal, magazine, e-zine, webzine, newsletter, or type of electronic serial publication which is available over the Internet." Chan, (1999). Smith (2003) defines e-journal as 'any journal that is available online, including both electronic only journals, and journals that are available both electronically and in print'. Bombak et al. (1992) define ejournal as 'a publication whose primary means of delivery to subscribers is through computer files.' E-journal is a serial publication like journal, magazine and newsletter in digital format and made available on CD-ROM, DVD, online systems and the Internet. E-journals are often referred to interchangeably as electronic publishing, electronic serials, online journals and electronic periodicals.

Within this broad definition, the titles can be electronically accessed using different technologies such as the World Wide Web (WWW), gopher, ftp, telnet, email, or listserv. This gives some structure and form of what the e-journal was, is, and will become. From the definition it is clear that e-journal is any periodical publication containing news or dealing with matters of current interest. It is an electronic format, to be displayed on a computer screen or a hand-held device.

3. Growth of E-Journal

The earliest e-journals started its journey from the late 1980s, in plain text format, and some of them can still be viewed in their original form today.

A good example of this early form of e-journal is 'Postmodern Culture', founded in 1990 and continuing to this day under the umbrella of Johns Hopkins University Press. This journal appeared just as the Internet was being established, as the culture was changing to allow mass viewing of material from home computers. It took advantage of the infant browsers – not yet capable of sophisticated interfaces or the presentation of multimedia content – and contributed to the development of an audience for journals which followed.

In the early 1990s there were still alternative technologies to the World Wide Web form of accessing content – ftp and gopher sites were popular, if primitive in the way they looked. They even had their own search engines: 'Archie' retrieved ftp content, 'Veronica' gopher sites. Archie and Veronica are no longer functional search engines, but Gopher survives along the much more sophisticated technology.

The internet originally is being seen as a medium for scientific and academic organizations to develop their global presence. A small but loyal popular audience for digital content was certainly developing. An Open Journals Framework Project report by Hitchcock et al stated that there were 115 e-journals in existence in 1995.

Later research by the same authors found an increase to 1,300 within the next three years. During these three years, academic institutions had taken on board the need to organize, evaluate and promote this content, through initiatives like the Super journal project. By early 2004 Leeds provided access to just over 12,000 titles, across all subject areas and including a large proportion of content which has never appeared in a printed, physical format. This brought its own administration issues such as organization and promotion, metadata, and training.

The growth of e-journal has been unprecedented and quite possibly unexpected in terms of publishing development. The situation becomes unmanageable without the knowledge and aptitude of serial management specialists within academic libraries. It is still the case that whatever the e-journal might achieve in technical excellence it does not yet have the long-term reliability to guarantee it permanence in the academic literature market. It will require considerable innovation and involvement by information specialists as well as commercial producers to ensure it achieves its promise so far. The growth of the e-journal in terms of sheer numbers has been staggering to witness, not only with the major publishers taking the strategic decision to digitise their content, but with the growth of innovative publishing models such as open access and open archiving.

4. What is Scholarly E-journal

For an academy, publishing a paper is an academic work. It is usually published as an academic journal. It contains original research results or reviews existing results. Such a paper is called an article. It will only be considered valid if it undergoes a process of peer review by one or more referees (who are academics in the same field). In order to check the paper is suitable for publication in the journal. A paper may undergo a series of reviews, edits and re-submissions before finally being accepted or rejected for publication. This process typically takes several months. Many academics offer a 'pre-print' copy of their paper for free download from their personal or institutional website.

Some journals, particularly newer ones, are now published in electronic form only. Paper journals are now generally made available in electronic form as well, both to individual subscribers, and to libraries. Almost always these electronic versions are available to subscribers immediately upon publication of the paper version, or even before. Sometimes they are also made available to non-subscribers after an embargo of two to twenty-four months, in order to protect against loss of subscriptions. Journals having this delayed availability are generally called delayed open access journals.

5. What is Peer review:

Peer review is a central concept for most academic publishing. Other scholars in a field must find a work sufficiently high in quality for it to merit publication. The process also guards against plagiarism.

6. What is Little e-journal

The ephemeral and popular forms of online digital content are considered as little e-journals. These popular models are the e-zine, webzine, and other less established forms of digital publication. The e-zine developed out of the culture of social print fanzines of the stapled and photocopied variety, and has become a fixture in the popular e-journal scene. These are often hobby or niche titles: for example the Free Directory of E-zines.

A main difference between the e-journal and e-zine is apart from its target audience. It is a lesser degree of content monitoring; where most e-journals have a peer review system to filter out unsuitable content. The e-zines generally have a more inclusive philosophy. In some subject areas this may be seen to be beneficial and to encourage a higher degree of debate and discussion.

The e-zine movement is a fast developing area, especially in creative areas such as writing, music, and popular culture. For some areas of research these publications may be just as valid as larger more established titles. The listserv started in the early days of the web when it was more likely to be referred to as a bulletin board. The listserv is a program that automatically redistributes e-mail to names on a mailing list. The bulletin board is an area of a web site where users can post messages for other users to read. Many of these have become as regulated and distinctive as journals of current interest.

A blog is basically a journal that is available on the web. Blogs are typically updated daily software. It allows people with little or no

technical background to update and maintain the blog. This is, in effect, a definition of an interactive e-journal. Some blogs, such as Open Access News, present themselves as a fully-fledged e-journal, with ISSN. They retain the general structure of a personal weblog. Internet Dictionary defines NetLingo as, "a frequent, chronological publication of personal thoughts and web links."

7. What are New publishing models:

New development in the world of e-journals is the open access movement. Institutional libraries are increasingly unable to fund journal title subscriptions. This is limiting the dissemination of academic research. The Association of Research Libraries-supported the principles were agreed including the use of electronic capabilities to provide wide access to scholarship.

The importance of copyright remaining with academic authors is to allow them to make their research available as widely as possible. There have been a number of new journals created, and much discussion in the academic and professional press. This then puts a new group of e-journals into the mix - strong, peer-reviewed titles with high-profile editorial boards. Initiatives such as SPARC, Public Library of Science and a recent collection of titles, the Directory of Open Access Journals are increasingly making an impact. The increase of open archiving of pre-prints and post-prints allow academics to make their work available to the widest possible audience. Open access of course works on the principle that all costs are covered by the authors or their institutions, rather than being a drain on departmental budgets through ever-rising subscriptions.

Free access e-journals may or may not fall into this model. It has been estimated by SHERPA that there are approximately 600 true open access titles. The number of freely-available titles on the web is much higher. These range from free online versions of subscription print titles; 'shop windows' with selected content of print titles; and true 'born digital' titles such as Electronic Journal of Sociology. There are also a number of smaller niche titles in subject areas such as media and fashion, and these take advantage of the new technology to the full. At present these journals are low impact but may well be attracting a sizable audience. They cannot be disregarded: indeed, with increased publicity to raise their impact factors, they could present a serious challenge to more commercial models.

8. What is Scholarly support:

The development of the e-journal as a central source and outlet for scholarly research, it is need to consider the pros and cons of the format, with particular emphasis on what the evolving medium means to the reader. Naturally, the print format remains core to student research, with the ease of photocopying, sharing information, and ease of browsing.

In favor of the digital publication are such advantages as more than one person able to view an article within a collection at the same time instant delivery of the journal on screen. It has the ability to quickly search content for specific points. It follows hyperlinks to other items of interest. The technological advances allowing additional information in a range of file formats to be incorporated into a published piece. Conversely, technology can not always been relied upon to deliver the exact results a reader might want; there can be server problems and broken hyperlinks. There may be a need for specific software to read articles, or article files may be corrupted or in hard-to-handle formats. There may be content in the printed journal excised from its electronic version. There is an assumption the reader has the technological expertise to browse and navigate content in several different interfaces. The e-journal has become slightly less complicated for the readers.

9. Future developments of E-journal

Professional librarians working in the field of e-journal management are interested in the technical developments. Digital content will become an accepted part of library budget or prohibit the development of adequate collections to support departmental research. The e-journal looks set to continue in its present 'journal' form for some time. There will be massive advances in multimedia capability and real-time interaction to develop a living archive of research material totally unprecedented in print journals of the past. Print of course will continue but there will an increase in 'electronic supplementary content'. It will also be the case that e-journal subscriptions will continue to exist independently of their print versions, allowing further development and innovation by editorial boards and academic contributors.

The development and take-up of digital television will necessarily have an impact on supporting written content available on text services

or the web. E-journals will have a knock-on impact on serial publications. Monograph texts too as e-books become the growth market of the 21st century for all groups of user. The e-journal looks set to continue as a healthy alternative to its print cousin, existing in tandem for the most part.

In the future 'born digital' content will continue to increase, gaining stature and acceptance amongst the likely contributors. The same contributors will embrace the philosophy of open archiving to obtain the largest possible coverage for their completed research. As student numbers increase within universities, courses outside of the traditional academic disciplines are likely to require a far wider spread of sources for teaching and research.

The more ephemeral formats will come. Interesting developments and debate will continue to brew on the more contentious aspects of digital publication, preservation, and propagation.

10 E- journals: Bangladesh Perspective

a. Subscription:

Information about electronic journals (e-journals) is required for their subscriber's management issues and necessities from the Bangladesh perspective. There is a need to establish a workable and sustainable consortium among libraries and information institutions in Bangladesh. Systematic efforts are needed urgently for the proper organization and management of e-journals.

E-journals are becoming popular and more effective with the growth and expansion of the Internet. They have revolutionized the change in the field of library and information services. They have been regarded as important library resources and many libraries all over the world have already replaced print journals with e-journals.

E-journals are not widely used in libraries and information centres in Bangladesh. Very few private universities and research libraries subscribe to ejournals in this country. Some leading public university libraries, for example Dhaka University Library, Rajshahi University Library, and Bangladesh University of Engineering and Technology (BUET) library are planning to subscribe to e-journals in the near future. It seems that the few libraries that are subscribing to e-journals are not aware of issues such as analysis of users needs, speed of Internet connection, adequate workstations with Internet connections in the library.

b. The pioneer e-journal subscribers in Bangladesh

1. Library and Information Service Unit (LISU) of International Center for Dhiarial Disease Research, Bangladesh (ICDDR) started subscription in 1994.
2. Subsequently, the leading private universities namely North South University Library,
3. Independent University, Bangladesh Library,
4. East West University Library,
5. American International University, Bangladesh Library came forward to subscribe e-journals.

Among libraries, institutions or organisations of Bangladesh that subscribe to ejournals many have sufficient computers. Some libraries have dedicated computers only for use in the library and some libraries do not have enough dedicated computers to access to e-journals in the library. The speed of Internet connection is not satisfactory in the present technical context of Bangladesh.

The libraries do not have dedicated speed allocation for access to e-journals in the libraries. Some libraries are not providing printing facilities, which is an essential service, because users prefer reading hard copy of articles to reading on screen. Sometimes the cost of printing is expensive and users are interested to write the downloaded articles into CD-ROM for further use at their convenience. Some libraries are not offering CD-writing facilities.

Some libraries, on their own initiatives, are offering training programmes for staff. The libraries indicated that no e-journals publishers are giving training facilities for the information professionals. Some library organization or institutions have web sites, but they do not provide links to e-journals and some do provide alphabetical listings of e-journals in their web sites. No library maintains a catalogue for e-journals. Only the British Council Library provides remote access to e-journals.

c. E-journals offer many advantages

1. E-journal keeps enormous resources to the collection;
2. E-journal saves libraries shelving space;
3. E-journal satisfy users' expectations for user friendly, convenient and remote access; and
4. E-journal provides powerful searching tools and features linking to more resources

Beside these the followings are the advantages:

a. Low cost: Bangladesh is a developing country where cost is always an important and a considerable factor. Usually print journals are very costly. Most of the libraries in Bangladesh cannot afford to subscribe print journals (foreign) or have to be very selective in their choice of subscription. Due to the low cost of e-journals, many libraries take the opportunity to subscribe to them. Also some e-journal publishers give discount price for the developing countries, which is usually not available for equivalent print.

b. No more missing: In print journal missing is really a big problem in Bangladesh. In many cases, publishers send the hard copy through postal service, which sometimes is not reached to the library. So this creates problem for both the subscriber (library) and the supplier (publisher). The hard copy of a journal can be missed from the library anytime. But in case of e-journals, such problems will not exist.

c. Timely reached: A print journal does not reach on time to library subscribers in Bangladesh. On the other hand, an e-journal reaches instantly to the user anywhere in the country if the Internet connection is available.

d. Multiple Accesses: In an institutional library multiple accesses to the resource are necessary. If a print journal is issued to a user, then no one else can access the journal in time. However, e-journals provide multiple access facility to users. This is a unique benefit of e-journal.

e. Wide search option: Indexing of journal articles is very essential. Unfortunately most of the libraries in Bangladesh do not have index of journal articles. So finding an article is laborious and it takes long time. On the other hand, e-journals provide wide search option (by author, title, key words, etc), so users can easily and quickly search and retrieve the desired articles.

f. Remote access: Remote access is one of the main features of e-journals. In Bangladesh where library opening hours is very limited. remote access to library resources can be good solution to meet the users need. Due to this, ejournals can be a good replacement of print journals.

g. Save physical space and human resources: E-journal saves shelving space in a library because it requires no space, thus it does not require human resources for shelving and rectification.

d. Disadvantages: E-journals have some disadvantages against print journals. The main problems and barriers are listed below:

a. Low bandwidth: Bangladesh has already been connected to the Information Super Highway through submarine fibre optic cables in 21 May 2006. However till date the benefits of the fibre optic cables have not reached to the users' level. The current bandwidth is not sufficient for the Internet dependent works in the country.

b. Lack of computers and computer user: Computers are becoming popular in Bangladesh, but the country is still lack of computers and computer literate users. Many senior researchers and educationists do not know how to operate the computer. This has led to them being not interested in using e-journals in the libraries.

c. Inadequate telephone connectivity: Bangladesh Telephone and Telegraph Board (BTTB) provide fixed-line service over the country which is inadequate. But as for Internet connection, most parts of the country depend on dial up connection where having a fixed telephone line is essential.

d. Lack of Internet connectivity and users: The country wide Internet users increasing. Still many organisations and libraries do not have any Internet connection, which is a vital barrier for e-journals subscription in Bangladesh.

e. Uninterruptible Internet connection: Bangladesh's dial up and broadband connection are frequently interrupted due to technological disruptions of Internet service provider.

f. High cost for infrastructure development: E-journals are less expensive than print journal. E-journal requires good infrastructure such as adequate number of workstations with Internet connection, high bandwidth, laser printers, dedicated web servers, Uninterruptible Power Supply (UPS). Many libraries cannot afford the high cost of this equipment.

g. No access after subscription period: The e-journal publishers / suppliers do not give access to the e-journals after the end of the subscription period, or do not provide the CD-ROM / DVD version of the journal.

h. Need continuous training and orientation: Prospective users of e-journals need orientation and training programmes frequently and it is the responsibility of the library to organize training programmes that require special resources person and proper planning.

i. Different search techniques: Search syntax and techniques are different from one publisher to another. So it is complicated for the users to

capture different search techniques of different journals and to know which search techniques are applicable for a particular e-journal site.

j. Bound to subscribe to unnecessary journals: When a library subscribes bundle of journals such as Emerald and JSTOR, usually they are bound to subscribe the entire journal in the sites. In many cases, some journals or some articles of the journals are not relevant to the user of the library or the organization. In Bangladesh so far, private universities are the main subscribers of e-journals and most of these universities offer only job oriented courses such as Business Administration, Computer Science and Engineering, Pharmacy, Law and Environmental Science, and do not offer basic courses like Physics, Chemistry and Biology. So the universities are paying for some unnecessary journals when they subscribe bundle of journal sites.

k. Need promotional activities: E-journals need promotional activities such as workshops conducted at regular intervals in order to promote the usage of ejournals. This is not so much required for the print journals. Therefore it is an extra work for the information professionals or the library to promote ejournal to prospective users.

11. Future of E-journals in Bangladesh

Bangladesh has 22 public and 54 private universities along with a large number of research institutions where journal is treated as a valuable part of higher education and research work.

As mentioned earlier, e-journals have some great advantages, which encourage some leading libraries to subscribe to e-journal. The subscription and use of e-journals in the libraries of Bangladesh will be increased day by day.

Telecommunications facilities are developing rapidly in Bangladesh especially after the approval of the government for the private sector investment. Currently existing mobile communication companies and land phone operators are working in this sector. It is expected the telecommunication infrastructure will go mass expansion and development; as a result, this enables the libraries and information institutions in the country to subscribe to e-journals efficiently. Almost 64 districts and considerable upazillas of Bangladesh have been brought under Internet coverage by BTTB through dial up connection.

Bangladesh Telegraph and Telephone Board (BTTB) are also providing high-speed Internet connection. It is also encouraging that

50% discount is applicable for the accredited universities, colleges, madrasas (religious institutions), as well as for training and research institutions. It has been mentioned earlier that Bangladesh is connected with international submarine fiber optic cable line, named South East Asia- Middle East-Western Europe-4 (SEA-ME-WE-4) cable system. It is expected that Bangladesh will receive a 10-gigabyte bandwidth and the cost for Internet connections will decrease which will encourage more libraries or organisations to take Internet connection. Ultimately, one of the main barriers for subscribing ejournal will be solved.

The University Grants Commission (UGC) of Bangladesh will come forward to make consortia among the public universities for subscribing e-journals. They will also provide financial and technological support to the public universities so that the universities can increase the quality of education and research work in their respective institutions.

12. Consortia or Buying Clubs in Bangladesh

Consortia or buying clubs have been established in most of the countries in the world to reduce the subscription cost of e-journals and to obtain some extra benefits from the publishers. In Bangladesh, not enough libraries are subscribing to e-journals in order to form a consortium. The Independent University, Bangladesh took initiative to form a consortium among the private universities in recent past. But no library has shown interest in establishing a consortium. If a consortium for e-journals in Bangladesh is established, the following benefits will be gained:

1. Most of the E-journal publishers offer special price for the consortia. So obviously, when a consortium is established by a good number of libraries, the subscription fee for a single library must be lower than the regular price.

2. More e-journals can be subscribed at the same cost.

3. It will help to establish resource sharing among the libraries.

4. Training facilities from the vendors or publishers utilizes the resources will be available.

A consortium for e-journal subscription involving the following:

a) All the public universities libraries of Bangladesh through the University Grants Commission of Bangladesh;

b) All the private universities who are offering similar courses or the same degrees; and

c) Research organisations working in similar fields.

13. E-Journal Opportunities

Electronic journals open up many opportunities and potentials for research and academic libraries. So the following action should be taken to enjoy the E-journal opportunities.

a. For an organizational subscription where number of users and e-journals are high, access through IP address should be confirmed. Library should start to subscribe to e-journals after obtaining approval from the e-journals authority to access through its registered IP address.

b. Before subscription of e-journals, library should ensure information and communication technology infrastructure such as high speed Internet connection, good number of workstations with Internet connection, laser printer, UPS, CD-writer, library's own website and dedicated web servers.

c. Library should provide remote and convenient access at anytime and from anywhere of the country where Internet is available. There is a number of software used all over the world to facilitate remote access to the user. Library should use such software to offer remote access opportunity to its user, which will encourage e-journals use.

d. Before and after the e-journals subscription, survey on users should be done at regular interval. Library should also receive information and suggestions from other libraries, which have already subscribed to the same journal.

e. Consortia or buying clubs should be established among the libraries in Bangladesh, which will not only ensure e-journals subscription at reduced a cost, but also give a suitable platform to share knowledge, conduct joint survey, and training programme.

f. Students in Bangladesh rely solely on books even at the university level. Faculty members should encourage students to read more journals, which will not only increase use of e-journals but also augment the standard of education.

g. According to copyright act, printing and CD-writing facilities at free of cost or reasonable price should be ensured for the best use of e-journal.

h. Library should organize training programme for the information professionals so that they can know about different search interface, latest changes of the journals site and develop sophisticated searching and retrieval skills or techniques.

i. Before subscription to e-journals, policy and procedure should be prepared and an expert should supervise the whole process.

j. Bandwidth of Internet connection must be increased and if it is not possible, dedicated speed should be allocated for access to e-journals.

k. The academic libraries depend on computer lab to give access to e-journals where the reading environment is very poor. So, it will be better if library can provide more computer workstations with Internet connection for access to e-journals.

l. Every library should have an own web site or the organizational web page. In the case of an organizational web page, the library's site must be included at the index page. For a quick and easy access, library should provide various types of e-journals lists, such as publisher, subject, and title (A-Z) list on the web page.

m. Libraries should maintain a catalogue of e-journals and the links should be provided to access to e-journals.

n. Every library that has Internet connection should select the most relevant free e-journals and should maintain a list on their websites.

E-journals, being relatively a new trend in the information world have generated a lot of debate over its access, storage, preservation and copyright. Due to the infrastructural problem in the field of library and information sector in Bangladesh, use and access to e-journals are very limited. But it is expected that e-journals will become more popular when each and every part of the country is connected with the world's Information Super.

Highway. By establishing a consortium or buying club, libraries can reduce subscription costs and obtain other related benefits. Libraries cannot ignore the e-journals, as it has now become a reality that many journals are now being published in an electronic format only.

14. E-journal Publication in Bangladesh

Bangladesh is also advancing in publishing e-Journals. In near future Bangladesh will achieve their goal in e-journal publication sector. In the mean time several Government organizations, department, universities, NGOs and private organization are publishing their E-journals. As for example some brief description are given here.

1. Bangladesh E-journal of Sociology:

Bangladesh Sociological Society is the publisher of this E-Journal. This e-journal is a guide to the Bangladeshi Sociologists and

Sociologists who are working in Bangladesh and are willing to register with society. They could use this page to get connected with other sociologist working on Bangladesh, academies all over the world. Members may deploy their works on the website, works displayed on the website free of cost for reasonable use. In order to offer greater coverage sociology in Bangladesh and work done by Bangladeshi Sociologist, the society will present research papers and articles in this web page for its international readers.

The first publication is volume-1, Number -1 was published in January 2004.

Volume 4. Number 1. January 2007
Volume 3. Number 2. July 2006
Volume 3. Number 1, January 2006
Volume 2. Number 2, July 2005
Volume 2. Number 1, January 2005
Volume 1. Number 2, July 2004
Volume 1. Number 1, January 2004

2. Daily News Papers:

Almost all the reputed National daily News Papers are published regularly in their website in electronic format. This is a great achievement of E-journal in Bangladesh.

3. Many Public and private sectors and NGOs published E-journal in their Web site. Some international organization published E-journal in their web site about Bangladesh.

4. Business Rationale for Investment on Power Operated Maize Sheller in Bangladesh

5. Agricultural Engineering International: the CIGR Ejournal.

6. Bangladesh Country Review

7. Bangladesh Economic Competitiveness

8. Bangladesh Economic Studies.

9. Daily news on Bangladesh and the region.

10. Portraits of Female Empowerment in Bangladesh

11. Bangladesh International Community News.

CHAPTER - 27

Internet Service Provider (ISP)

1. What is Internet Service Provider (ISP)

Internet Service Provider (ISP) is a service provider of internet access. It is also called Internet Access Provide (IAP). In the past, most ISPs were run by the phone companies. Now, ISPs can be started by any individual or group with sufficient money and expertise of ICT. Internet sevice providers use various technologies such as dial-up and DSL. They may provide a combination of services including Internet transit, domain name registration and hosting, web hosting, and colocation.

2. Definition of ISP or IAP

According to Wikipedia, the free encyclopedia, "An Internet service provider (abbr. ISP, also called Internet access provider or IAP) is a business or organization that provides to consumers access to the Internet and related services."

3. ISPs Technological aspects:

ISPs use different technologies to enable consumers to connect to their network. For Home users, the most popular technical options are

1. dial-up,

2. DSL (typically ADSL).
3. Broadband wireless access.
4. Cable modem, and
5. ISDN (typically BRI).

For customers who have more demanding requirements, such as medium-to-large businesses, or other ISPs, the technical options are

1. DSL (often SHDSL or ADSL),
2. Ethernet,
3. Metro Ethernet,
4. Gigabit Ethernet,
5. Frame Relay,
6. ISDN (BRI or PRI),
7. ATM,
8. Satellite Internet access and
9. SONET.

With the increasing popularity of downloading music and online video and the general demand for faster page loads, higher bandwidth connections are becoming more popular.

a. How ISPs connect to the Internet

ISPs customers pay them for Internet access. ISPs themselves pay upstream ISPs for Internet access. In the simplest case, a single connection is established to an upstream ISP using one of the technologies described above. The ISP uses this connection to send or receive any data to or from parts of the Internet beyond its own network. The upstream ISP uses its own upstream connection, or connections to its other customers (usually other ISPs) to allow the data to travel from source to destination.

The technical situation is often more complicated. For example, ISPs with more than one Point of Presence (PoP) may have separate connections to an upstream ISP at multiple PoPs or they may be customers of multiple upstream ISPs. They have connections to each

one at one or more of their PoPs. ISPs may engage in peering, where multiple ISPs interconnect with one another at a peering point or Internet exchange point (IX), allowing the routing of data between their networks, without charging one another for that data - data that would otherwise have passed through their upstream ISPs, incurring charges from the upstream ISP. ISPs that require no upstream, and have only customers and/or peers, are called Tier 1 ISPs, indicating their status as ISPs at the top of the Internet hierarchy. Routers, switches, Internet routing protocols, and the expertise of network administrators all have a role to play in ensuring that data follows the best available route and that ISPs can see one another on the Internet.

b. What is Virtual ISP (vISP)

A Virtual ISP (vISP) is not self operated ISPs. It purchases services from another ISP (sometimes called a wholesale ISP or similar within this context). They allow the vISP's customers to access the Internet via one or more Points of Presence (PoPs) that are owned and operated by the wholesale ISP. There are various models for the delivery of this type of service. For example, the wholesale ISP could provide network access to end users via its dial-up modem PoPs or DSLAMs installed in telephone exchanges, and route, switch, and/or tunnel the end user traffic to the vISP's network, whereupon they may route the traffic toward its destination.

In another model, the vISP does not route any end user traffic, and needs only provide AAA (Authentication, Authorization and Accounting) functions, as well as any value-add services like email or web hosting. Any given ISP may use their own PoPs to deliver one service, and use a vISP model to deliver another service, or, use a combination to deliver a service in different areas. The service provided by a wholesale ISP in a vISP model is distinct from that of an upstream ISP, even though in some cases, they may both be one and the same company. The former provides connectivity from the end user's premises to the Internet or to the end user ISP, the latter provides connectivity from the end user's ISP to all or parts of the rest of the Internet.

A vISP can also refer to a completely automated white label service offered to anyone at no cost or for a minimal set-up fee. The actual ISP

providing the service generates revenue from the calls and may also share a percentage of that revenue with the owner of the vISP. All technical aspects are dealt with leaving the owner of vISP with the task of promoting the service. This sort of service is however declining due to the popularity of unmetered internet access also known as flatrate.

c. What is Broadband Internet Access

Broadband Internet access is termed as broadband internet or broadband. Broadband is a high data-transmission rate Internet connection. DSL and cable modem, both popular consumer broadband technologies, are typically capable of transmitting faster than a dial-up modem (56 kbit/s (kilobits per second). Broadband Internet access became a rapidly developing market in many areas. Modem consumer broadband implementations, up to 30 Mbit/s, are several hundred times faster than those available at the time the Internet first became popular (such as ISDN and 56 kbit/s) while costing less than ISDN and sometimes no more than 56 kbit/s, though performance and costs vary widely between countries. Broadband in this context refers to the relatively high available bitrate, when compared to systems such as dial-up with lower bitrates, which could be referred to as narrowband.

Broadband in telecommunications is a term which refers to a signaling method. This includes or handles a relatively wide range of frequencies which may be divided into channels or frequency bins. Broadband is always a relative term, understood according to its context. The wider the bandwidth, greater is the information carrying capacity. In radio, for example, a very narrow-band signal will carry Morse code; a broader band will carry speech; a still broader band is required to carry music without losing the high audio frequencies required for realistic sound reproduction. A television antenna described as normal may be capable of receiving a certain range of channels; one described as broadband will receive more channels. In data communications a modem will transmit a bandwidth of 64 kilobits per seconds (kbit/s) over a telephone line; over the same telephone line a bandwidth of several megabits per second can be handled by ADSL, which is described as broadband.

Broadband in data communications may have the same meaning as above, so that data transmission over a fiber optic cable would be referred

to as broadband as compared to a telephone modem operating at 600 bits per second. Broadband in data communications is frequently used in a more technical sense to refer to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission, regardless of actual data rate. In network engineering this term is used for methods where two or more signals share a medium.

Various forms of Digital Subscriber Line (DSL) services are broadband in the sense that digital information is sent over one channel and voice over another channel sharing a single pair of wires. Analog modems operating at speeds greater than 600 bit/s are technically broadband. They obtain higher effective transmission rates by using multiple channels with the rate on each channel limited to 600 baud. For example, a 2400 bit/s modem uses four 600 baud channels. This is in contrast to a baseband transmission where one type of signal uses a medium's full bandwidth such as 100BASE-T Ethernet.

Ethernet, however, is the common user interface even to DSL data links. Ethernet provisioned over cable modem often is a competitive alternative to DSL, especially in the small office or market. Users who need more than DSL or cable modem speeds will often use metro ethernet. It is often more expensive (per megabit) than T-carrier (or E-carrier in appropriate parts of the world, or Asynchronous Transfer Mode. Metro ethernet is usually implemented over a metropolitan all-optical network

D. What is Multiplexing

Communications may utilize a number of distinct physical channels simultaneously. This is multiplexing for multiple access. These channels may be distinguished as follows:

1. Time Division Multiplexing Access or (TDMA), separated from each other in time,
2. Frequency Division Multiplexing Access (FDMA), separated each other in carrier frequency
3. Wavelength Division Multiplexing Access (WDMA) separated each other in wavelength, or
4. Code Division Multiple Access (CDMA) in access method.

Each channel that takes part in such a multiplexing exercise is by definition narrowband whereas the whole set of channels taken together and utilized for the same communication could be described as broadband.

e. What is Wireless Broadband

Wireless Broadband is a fairly new technology that provides high-speed wireless internet and data network access over a wide area. Broadband means 'having instantaneous bandwidth greater than around 1 MHz and supporting data rates greater than about 1.5 Mbit/s'. Wireless Broadband features speeds are roughly equivalent to wired broadband access. Many Wireless Broadband services provide average download speeds of over 100 Mbit's. and are estimated to have a range of 50 km (30 miles). Technologies used include LMDS and MMDS, and one particular access technology is being standardized by IEEE 802.16, also known as WiMAX.

At first, Wireless Internet Service Providers (WISPs) were only found in rural areas not covered by cable or DSL. These early WISPs would receive a large connection, such as a T1 or DS3 connection, and then prodcast signal from a high elevation, such as at the top of a water tower. To receive this type of internet, consumers would mount a small dish to the roof of their home or office and point it to the transmitter.

f. What is Mobile Wireless Broadband

Wireless Broadband technologies include new services from companies such as Verizon, Sprint, and Cingular. This technology allows a more mobile version of this broadband access. Consumers can purchase a PC-card, laptop-card, or USB equipment to connect their PC or laptop to the internet via cell-phone towers. This type of connection would be stable in any area that could also receive a strong cell-phone connection.

g. Voice over Internet Protocol (VoIP) in Bangladesh

Voice over Internet Protocol denotes as VoIP. It is the technical system through which international telephone call can be done by using internet protocol (IP). By using this call rate is very low. So this is popular among the users.

Mobile operator, PSTN and ISPs provide VoIP service. Three things are required for VoIP service.. These are -

1. An internet connection.
2. A telephone line. and
3. An international carrier.

1. VoIP through ISPs

Mobile operators as well as PSTN can obtain internet service from any ISP. The Government has to rely on their reporting to calculate its share of revenue. On the other hand, if the ISPs are allowed to VoIP, they will receive voice traffic from overseas and will terminate those calls to any Mobile/PSTN network. As such the government has two sources of documents through which they can verify traffic, the ISPs themselves and the telephone company from which the 'E1 line' is taken. In short ensuring government's fair share of revenue from VoIP would become much easier if licenses are given to only ISPs. A central CDR Server (which does not cost much) is to be placed in any suitable location for calculating and verifying VoIP traffic volume of all licensees. In this context, it is clearly understood that there is no requirement of common platform for immediate legalization of VoIP.

Issuing VoIP license to only ISPs is the way to make sure that all three business industries are benefited from the technological blessing. As mentioned before, the ISPs must have the aid of a telephone service provider as they are the only industry without a last mile end. As such, the phone operator will also be benefited from this technology as they will be charging their customers with the call. Every single call originates from/ terminates to any of Mobile/PSTN phone line. And the government will have two sources of income, one, from the VoIP license owner and another, VAT from the phone operator per call. This is the only way to ensure everyone wins.

2. VoIP through VSAT

Present capacity of SEA-ME-WE-4 is limited and may not fulfill the bandwidth requirement once the VoIP legalized. In order to give the immediate benefit, VoIP through VSAT network can be approved. Simply because of cost-benefit VoIP licensees will use Submarine

bandwidth once it is available. And thus, due to lack of trouble free Submarine Bandwidth, the licensing procedure should not be delayed.

3. Legal aspect of VoIP

It is a common practice worldwide to separate international call traffic from local call traffic. It makes monitoring easier for the government. The only way to do this for VoIP in Bangladesh is to issue license to deserving companies who have the technological facilities. Issuing VoIP license is a matter of policy of the Government. So this matter should be decided as per international telecommunication practice and the interest of the public where the better service will be available at lower cost. Telecom industry is a large multinational industry in the country and it will be foreign companies who will be benefited if tacos are awarded VoIP license. ISP industry is truly a local industry, and if they earn revenues from this technology, the money stays in the country as income of a local company. To take any decision about the licensing of VoIP the public interest should be taking into account. Currently BTRC has planned to issue VoIP license to Mobile phone operators, PSTN (Public Switched Telephone Network) Operators and to ISPs.

VoIP businesses were running illegally. It should be stopped. But VoIP business is good for public. They get the better service with lower price. The technological development should be encouraged. If the VoIP industry legalized under the legal framework this industry will be develop and it will generate employment. It is fair practice that the VoIP technology will be legalized by bringing it under the legal frame work as soon as possible.

4. ISP Industry & ICT in Bangladesh

The 11 year old industry has given its best effort in developing the ICT sector of Bangladesh. This industry is composed of mostly young entrepreneurs employing thousands of hard-working talents of Bangladesh. ISPs are a growing industry of ICT sector in Bangladesh.

a. History of Bangladesh ISP Industry

Bangladesh had access to email via dialup to Bulletin Board Systems (BBS) of a few local providers in the early 90s. The combined

Internet users of all the email-only service providers were not more then 500. Users were charged by the kilobyte, and mail was transferred from the BBS service providers to the rest of the world by International dialup using UUCP.

Bangladesh Government allowed VSAT's to be operated in the Private Sector in June 1996, allbeit to be provided solely by the Government owned Telephone Operator, BTTB. Only a handful of ISPs were connected within the first year. However, more liberal Government policies followed in the subsequent years which led to a rapid expansion of this industry, eventually resulting in over 180 registered ISP's by 2005. ISPs are currently regulated by the Bangladesh Telecommunication Regulatory Commission through the Bangladesh Telecommunications Act.

b. ISP ASSOCIATION BANGLADESH

The Internet Service Providers Association of Bangladesh (ISPAB) was organized in the year 1998. The object of the ISPAB is to improve business conditions of Internet Service Providers operating in Bangladesh. The activities of ISPAB are as follows:

1. To serve the common business interest of its Members by promoting higher business standards; disseminating technical, legal and other information to its members;
2. To operate as a trade association for the benefit of the community of Internet Service Providers in the Bangladesh, and their customers;
3. To work for the enactment of laws and rules advancing the common business interests of its Members; and
4. Performing such other function as are customary among trade associations.

The Internet Service Providers Association of Bangladesh (ISPAB) strongly supports the government's recent decision to legalize VoIP (Voice over Internet Protocol). The decision to issue VoIP licenses could not have been made any sooner, and it is strongly believe that this initiative to embrace this wonderful technology will benefit our economy in every way. Although it is highly appreciated the effort of government to make overseas calls easier for the public, by reducing

the charges to a minimum amount, the fact of the matter is that a traditional phone call can never be as cheap as VoIP. since VoIP uses the internet to carry voice and other digital information through packets. We are all aware that there is a huge demand for VoIP service in this country. It is cheap, and as it transmits voice communication, it can be used by both the literate and illiterate population. Thus, whether people like it or not, the huge demand for this technology drives a sizable illegal business. The government is cheated out of their share of the revenue. Therefore, legalizing VoIP in the soonest possible time is imperative. It will not only boost the economy of our country, but will also help citizens home and abroad at a personal level, as they will be able to communicate with their families cheaply.

5. Legal Basis of ISP

a. The Telegraph Act 1885.

b. The Wireless Telegraphy Act 1933

c. The Bangladesh Telegraph and Telephone Board Ordinance 1979.

d. The Bangladesh Telecommunication Act 2001.

CHAPTER - 28
Electronic Media

1. What is E-Electronic Media

Electronic media may be termed as E-media. It is the media that utilize electronics or electromechanical energy to access the content by the end user (audience). The primary electronic media sources familiar to the general public are better known as video recordings, audio recordings, multimedia presentations, slide presentations, CD-ROM and Online Content.

The term is usually associated with content recorded on a storage medium. The recordings are not required for live broadcasting and online networking. Any equipment used in the electronic communication process e.g. radio, television, telephone, desktop computer, game console, handheld device, may also be considered electronic media.

Electromechanical devices are less expensive and more effective. A standard integrated circuit and write a computer program to carry out the same task through logic. Transistors have replaced almost all electromechanical devices, are used in most simple feedback control systems, and appear in huge numbers in everything from traffic lights to washing machines.

Electronic media devices have found their way into all parts of modern life. The term is relevant to media ecology for studying it's impact compared to printed media. It has been broadening the scope of understanding media beyond a simplistic aspect of media such as one delivery platform e.g. the World Wide Web (W.W.W.). The term is also relevant to professional career development regarding related skill sets.

Most new media are in the form of digital media. However, electronic media may be in either analog or digital format.

2. Kinds of media

Electronic Media broadly can be classified as-

a. Multimedia,

b. Mass Media,

c. Print Media, and

d. New Media.

a. Multimedia:

Multimediaia is media that uses multiple forms of information content and information processing (e.g. text, audio, graphics, animation, video, interactivity) to inform or entertain the audience. Multimedia also refers to the use of electronic media to store and experience multimedia content. Multimedia is similar to traditional mixed media in fine art, but with a broader scope. The term rich media is synonymous for interactive multimedia. Multimedia means that computer info can be represented through audio, graphics, image, video and animation in addition to traditional media. Hypermedia can be considered one particular multimedia application.

The use of different media to convey information; text together with audio, video, graphics and animation, often packaged on CD-ROM with links to the Internet. Multimedia is relating to the combined use of media. It is also relating to an application that can combine such media into an integrated package

b. Mass media

The communications media, especially radio, television, and newspapers that reach the mass of the people is called mass media. Mass Media can be classified as-

1. Print Media,

2. Electronic Media.

a. Radio (Audio Broadcast),

b. Television (Video Broadcast), and

c. E-Journal and E-book

d. New media

c. Print media

Print media is a process for production of texts and images, typically with ink on paper using a printing press. It is often carried out as a large-scale industrial process, and is an essential part of publishing and transaction printing.

2. Electronic Media.

a. Radio (Audio Broadcast)

Radio (Audio Broadcast) is an electronic mass media. It comprises with Audio Transmitter to transmit the Audio signal and receive by radio. It is a very popular and affective mass media. The transmission of audio signal started from radio stations and the people receive the signal within the area covered by the power of the transmitter.

Distribution methods of Audio Broadcast

a. Terrestrial radio modulation: AM | FM | COFDM

b. Frequency allocations: LW | MW (MF) | SW (HF) | VHF

c. Hidden signals: AMSS | DirectBand | RBDS

d. Codecs: AAC | Musicam

e. Terrestrial digital audio broadcasting systems: DAB |

f. DAB+ | DRM | HD Radio

g. Earth Orbital digital audio broadcasting systems: Sirius WorldSpace / XM

h. Digital radio / Audio processing .

b. Television (Audio-Video Broadcast)

Television (Video Broadcast) is also a powerful electronic mass media. It is comprises with Audio-Visual Transmitter to transmit the

signal and received by the Television sets. The signal transmits from the Television station and the public received the signal within the area covered by the power of the transmitter or the network covered by the television stations.

A television station is a type of broadcast station that broadcasts both audio and video to television receivers in a particular area. TV stations made their broadcasts by sending specially encoded radio signals over the air, called terrestrial television. Individual television stations are usually granted licenses by a government agency to use a particular section of the radio spectrum (a channel) through which they send their signals. Some stations use LPTV broadcast translators to retransmit to further areas. Television stations are now in the process of converting from analogue (NTSC, PAL, or SECAM) to digital TV (ATSC, DVB, or ISDB).

Television channel

The term television channel generally refers to either a television station or its cable / satellite counterpart. Sometimes, it is confused with the term television network, which describes a group of geographically-distributed television stations that share affiliation/ownership and some or all of their programming with one another. On digital platforms, such channels are usually arbitrary, due to virtual channels. Cable network is the most common colloquial term for a television channel available via cable television. Such channels are usually also available via satellite television, including direct broadcast satellite providers such as DirecTV. Alternative terms include cable channel, non-broadcast network, or programming service, the latter being mainly used in legal contexts.

c. E-Journal and E-book

E-Journal and E-book is also a strong mass media that are published in World Wide Web (www). This publication can be read through internet. Some are freely accessible and some are accessible on payment. This becomes a popular affective mass media in the time coming.

d. New media

New media refers to new forms of human and media communication that have been transformed by the creative use of technology to fulfil the same basic social need to interact and transact. New media is also closely associated with the term "Web 2.0" which

refers to a proposed second generation of Internet-based services - such as social networking sites and wikis - that emphasise online collaboration and sharing among users. The technologies for new media have been in existence for decades. In recent years these technologies have grown intuitive enough for people. With innovative uses of new media has resulted in its popularity today.

Analog signal

An analog or analogue signal is any variable signal continuous in both time and amplitude. It differs from a digital signal. Analog is usually thought of in an electrical context, however mechanical, pneumatic, hydraulic, and other systems may also convey analog signals. Electrically, the property most commonly used is voltage followed closely by frequency, current, and charge. Any information may be conveyed by an analog signal, often such a signal is a measured response to changes in physical phenomena, such as sound, light, temperature, position, or pressure, and is achieved using a transducer.

3. What is Broadcasting

Broadcasting is the distribution of audio and/or video signals which transmit programs to an audience. The audience may be the general public or a relatively large sub-audience, such as children or young or adults. There is wide variety of broadcasting systems. They have different capabilities. Such as-

1. The largest broadcasting systems are institutional public address systems, which transmit nonverbal messages and music within a school or hospital,

2. Low-powered broadcasting systems which transmit radio stations or television stations to a small area.

3. National radio and television broadcasters have nationwide coverage, using retransmitted towers, satellite systems, and cable distribution.

4. Satellite radio and television broadcasters can cover even wider areas, such as entire continents, and

5. Internet channels can distribute text or streamed music worldwide.

The sequencing of content in a broadcast is called a schedule. As with all technological endeavors, a number of technical terms and slang have developed. Television and radio programs are distributed through

radio broadcasting or cable, often both simultaneously. By coding signals and having decoding equipment in homes, the latter also enables subscription-based channels and pay-per-view services.

The term broadcast was coined by early radio engineers from the midwestern United States. Broadcasting forms a very large segment of the mass media. Broadcasting to a very narrow range of audience is called narrowcasting.

Broadcasters may rely on a combination of these business models. For example,

1. National Public Radio,
2. A non-commercial network within the United States,
3. Receives grants from the Corporation for Public Broadcasting by public membership,
4. By selling extended credits to corporations.

Broadcast are generally two types.

a. Recorded broadcasts, and

b. live broadcasts:

a. Recorded Broadcasts

This allows correcting errors, and removing superfluous or undesired material, rearranging it, applying slow-motion and repetitions, and other techniques to enhance the program. A disadvantage of recording first is that the public may know the outcome of an event from another source, which may be a spoiler

b. Live broadcasts

Live events like sports telecasts can include some of the aspects including slow motion clips of important goals / hits etc in between the live telecast. Many events are advertised as being live, although they are often recorded live. This is particularly true of performances of musical artists on radio when they visit for an in-studio concert performance. This intentional blurring of the distinction between live and recorded media is viewed with chagrin among many music lovers. Similar situations have sometimes appeared in television

4. What is Broadcast license

A broadcast license is a specific type of spectrum license that grants the licensee the right to use a portion of the radio frequency

spectrum in a given geographical area for broadcasting purposes. Licensing is typically performed by government agencies, providing a mechanism both for managing the limited resource of radio frequency spectrum and for implementing prevailing public policy, such as policies regarding concentration of media ownership. Management of technical specifications, such as those implemented in broadcast television systems, is normally undertaken as a part of broadcast licensing in each country.

5. Economic Value of frequency spectrum

Originally, broadcast licenses were issued for only a nominal payment, but work by economist Ronald Coase developed a theory that broadcast licenses in a spectrum that was limited had high economic value, which could and should be paid for on the open market. Increasingly, spectrum licenses are offered via spectrum auctions.

6. Allocation of Radio ,TV and TV channel frequencies

The frequencies assigned to broadcast Radio and Television channels in various regions of the world, along with the ITU letter designator for the system used. The frequencies shown are for the video and audio carriers. The channel itself occupies frequency of several megahertz of the bandwidth. For example, North American channel 2 occupies the spectrum from 54 to 60 MHz.

7. Broadcast network

A broadcast network is an organization, such as a corporation or other association. It provides live or recorded content, such as movies, newscasts, sports, and public affairs programs for broadcast over a group of radio or television stations. They are generally primarily either a television network or a radio network, although some organizations run both types of networks.

8. Community Radio / Television Broadcast

Community Television is a form of Citizen Media like Public Access Radio / Television and the Community Channel. In principle, community television is another model of facilitating media production and involvement by private citizens. Australia has a special type of broadcasting license for community television. Holders of such a license must conform to various rules, primarily relating to advertising and to a lesser extent, program content. There are a number of stations

and distributors that release the same sort of content with other types of license, or none at all. The Australian TV stations with community licenses are located in Adelaide, Brisbane, Lismore, Melbourne, Mount Gambier, Perth, Sydney and nearly 100 remote Aboriginal communities. In Brisbane, Melbourne, Perth, Sydney and the remote communities, the stations have ongoing licenses. The stations in Adelaide, Lismore and Mount Gambier currently have trial licenses.

Community Radio / Television programs are most often made by amateurs about their own communities and special and diverse interests. In other cases, companies produce the programs. Community Radio / TV is funded by a mixture of sponsorship, subscriptions and donations, membership fees, grants, merchandise sales and sale of air time to program providers. It receives no regular national government funding. Many programs are paid for by the producers themselves. A special emphasis of community TV is the provision of programs in an increasing range of community languages and about community cultures. Over twenty languages groups, many from newly migrant and refugee communities are broadcast regular by the CRadio/CTV stations.

9. Terrestrial Television Broadcast

Terrestrial televisions are known as Over-The-Air (OTA), free TV, or broadcast television. It is the traditional method of television broadcast before the advent of cable and satellite television. In some countries and many densely-populated areas it is decreasing in use but in others, digital terrestrial has become popular. Terrestrial television broadcasting was the only television media itself. There was virtually no other method of television broadcasting until the 1950s

10. Satellite Television Broadcast

Satellite television is television delivered by way of communications satellites, as compared to conventional terrestrial television and cable television. In many areas of the world satellite television services supplement older terrestrial signals, providing a wider range of channels and services, including subscription-only services.

Bangladesh Satellite televisions stations are

1. Bangla Vision,
2. NTV,
3. RTV,

4. ATN Bangla,
5. Channel I,
6. Channel 1,
7. Boishaki TV,
8. ETV,
9. DESH TV,
10. Digonto TV,
11. Islamic TV etc.

11. Cable Television Broadcast

The abbreviation CATV is often used to mean Cable TV. Cable television is a system of providing television to consumers via radio frequency signals transmitted to televisions through fixed optical fibers or coaxial cables as opposed to the Over-The-Air (OTA) method used in traditional television broadcasting. FM radio programming, high-speed Internet, telephony and similar non television services may also be provided. It originally stood for Community Antenna Television. Cable television's origins in 1948 in areas where over-the-air reception was limited by mountainous terrain, large community antennas were constructed, and cable was run from them to individual homes.

12. Internet radio / e-Radio Broadcast

Internet radio denotes e-Radio is an audio broadcasting service transmitted via the Internet. Broadcasting on the Internet is usually referred to as webcasting. It is not transmitted broadly through wireless means. It is delivered over the World Wide Web. The term e-Radio suggests a streaming medium that presents listeners with a continuous stream of audio to which they have no control much like traditional broadcast media. It is not synonymous with podcasting which involves downloading and therefore copyright issues. Many Internet radio stations are associated with a corresponding traditional terrestrial radio station or radio network. Internet-only radio stations are usually independent of such associations.

Internet radio stations are usually accessible from anywhere in the world—for example, to listen to an Australian station from Europe or America. This makes it a popular service for expatriates and for listeners with interests not adequately served by local radio stations. Some Internet radio services offer news, sports, talkback, and various

genres of music—everything that is on the radio station being simulcast over the internet with a netcast stream.

13. Legal Aspect of Broadcast

a. Federal Radio Commission

The Federal Radio Commission (FRC) was a government body that regulated radio use in the United States from its creation in 1927 until its replacement by the Federal Communications Commission (FCC) in 1934. The Commission was created to regulate radio use "as the public convenience, interest, or necessity requires." The Radio Act of 1927 superseded the Radio Act of 1912, which had given regulatory powers over radio communication to the Secretary of Commerce and Labor. The Radio Act of 1912 did not mention broadcasting and limited all private radio communications to what is now the AM band.

b. The Radio Act of 1927

Prior to 1927, radio was regulated by the United States Department of Commerce, and Commerce Secretary Herbert Hoover played a strong role in shaping radio. His powers were limited. He was not allowed to deny broadcasting licenses to anyone who wanted one. The result was that many people perceived the airwaves to suffer from "chaos," with too many stations trying to be heard on too few frequencies. (Initially only two frequencies were available for broadcasting with one of these being reserved for "Crop reports and weather forecasts") After several failed attempts to rectify this situation, Congress finally passed the Radio Act of 1927 (signed into law February 23, 1927), which transferred most of the responsibility for radio to a newly created Federal Radio Commission. (Some technical duties remained the responsibility of the Radio Division of the Department of Commerce.)

The five-person FRC was given the power to grant and deny licenses, and to assign frequencies and power levels for each licensee. The Commission was not given any official power of censorship, although programming could not include "obscene, indecent, or profane language." In theory, anything else could be aired. In practice, the Commission could take into consideration programming when renewing licenses and their ability to take away a broadcaster's license obviously enabled them to control content to some degree. Some key examples are listed below.

The Commission also had little power over networks; in fact, the Radio Act of 1927 made almost no mention of the radio networks (notably NBC and, a bit later CBS) that were in the process of dominating radio. The only mention of radio networks was vague: The Commission (the Federal Radio Commission) shall "Have the authority to make special regulations applicable to stations engaged in chain broadcasting."

The act did not authorize the Federal Radio Commission to make any rules regulating advertising. Advertising was mentioned in the act with only slightly more authority than networking; merely requiring advertisers to identify themselves:

All matter broadcast by any radio station for which service, money, or any other valuable consideration is directly paid, or promised to, or charged to, or accepted by, the station so broadcasting, from any person, firm, company, or corporation, shall at the time the same is so broadcast, be announced as paid for or furnished as the case may be, by such person, firm, company, or corporation.

A forerunner of the "equal time rule" was stated in section (18) of the Radio Act of 1927 which ordered stations to give equal opportunities for political candidates. The act did vest in the Federal Radio Commission the power to revoke licenses and give fines for violations of the act.

The Radio Act of 1927 divided the country into five geographical zones. Each zone was represented by one of the five Commissioners. The 1928 reauthorization of the Radio Act included a provision, called the "Davis Amendment" after its sponsor Ewin L. Davis that required each zone to have equal allocations of licenses, time of operation, station power, and wavelength. This greatly complicated things for the Commissioners; they were required to deny station applications to otherwise qualified candidates simply because the new station would put a particular state or zone over its quota. For example, the northeast had a greater population than the southwest, but was limited to the same number of stations as more sparsely populated areas. Likewise, many small communities in the southwest could have added a local station without increasing interference (because of their remoteness), but were prevented from doing so by the Davis Amendment.

Although the Commission's primary responsibility was radio, on February 25, 1928 Charles Jenkins Laboratories of Washington,

DC became the first holder of a television license from the Federal Radio Commission.

c. Formation of the Federal Radio Commission

President Calvin Coolidge nominated five men to the commission, Admiral W.H.G. Bullard as chairman, Colonel John F. Dillon, Eugene O. Sykes, Henry A. Bellows, and Orestes H. Caldwell. The first three were confirmed by the Senate and the first two died soon afterward. Bellows and Caldwell didn't receive salaries, but stayed on anyway. These three did conduct a badly needed reallocation of frequencies. In October, President Calvin Coolidge removed Bellows from the commission; he returned to Minneapolis where he had been a broadcaster. In November 1927 Harold Lafount and Sam Pickard joined the commission. In March 1928 Caldwell was barely re-confirmed and Ira Robinson became chairman, the commission was finally complete.

d. Radio licensing

In the spring of 1928, the commissioners made drastic reallocations and told 164 stations to justify their existence or be forced to stop broadcasting (these hearings came under the title of General Order 32). Many low-powered independent stations were eliminated, although eighty-one stations did survive, most with reduced power. Educational stations fared particularly poorly. They were usually required to share frequencies with commercial stations and operate during the daytime, which was considered worthless for adult education.

e. Other accomplishments

The FRC carried out provisions of the Radio Act of 1927 to license persons operating amateur and commercial transmitters. It also complied with new treaty obligations to assign U.S. stations ITU prefixes.

f. Controversy

When broadcasting began to be regulated, and stations had to have a broadcast license, some saw this as an infringement of the First Amendment to the United States Constitution stating that the government shall not stop freedom of speech in the media. This was because prior to broadcast licensing; anyone could start transmitting their views cheaply and efficiently.

Almost from the start, the FRC was accused of being captured by the industry it regulated by radio broadcasters. Historians and contemporary critics who held this position generally pointed to the results of FRC regulation which, in many cases, advantaged large commercial radio broadcasters at the expense of smaller noncommercial broadcasters. Early radio regulation has since become a commonly-used example of rent-seeking.

g. Abolishment of the Federal Radio Commission

In 1934 Congress passed the Communications Act, which abolished the Federal Radio Commission and transferred jurisdiction over radio licensing to a new Federal Communications Commission. Title III of the Communications Act contained provisions very similar to the Radio Act of 1927, and the new FCC largely took over the operations and precedents of the FRC.

h. Radio network

A radio network is a network system which distributes programming to multiple stations simultaneously or slightly delayed, for the purpose of extending total coverage beyond the limits of a single broadcast signal. The resulting expanded audience for programming essentially applies the benefits of mass-production to the broadcasting enterprise.

Most radio networks also produce much of their programming. Originally, radio networks owned some or all of the radio stations that broadcast the network's programming. Presently however, there are many networks that do not own any stations and only produce and/or distribute programming. Similarly station ownership does not always indicate network affiliation. A company might own stations in several different markets and purchase programming from a variety of networks.

Radio networks rose rapidly with the growth of regular broadcasting of radio to home listeners in the 1920s. This growth took various paths in different places. In Britain the BBC was developed with public funding, in the form of a broadcast receiving license, and a broadcasting monopoly in its early decades. In contrast, in the United States of America various competing commercial networks arose funded by advertising revenue. In that instance, the same corporation that owned or operated the network often manufactured and marketed the listener's radio.

CHAPTER- 29
Computerization in Bangladesh

1. **Computerization in Bangladesh**
   - **a. Innovation of Bangla software**
   - **b. Use of Internet and e-mail**
   - **c. Computer assembling**
   - **d. Use of computer**
   - **e. Computer organizations**
   - **f. Computer education**
2. Localization of computer : Initiatives and Achievements
   - **a. What is Localization of computer :**
   - **b. Development of Localization in Bangladesh**
   - **c. Achievement in OSS (Open Source Software) localization**
   - **d. What is Open content development?**
   - **e. Bangla Wikipedia development**
   - **f. Future development**

---

1. Computerization in Bangladesh

In 1960s Bangladesh entered into the computer world. The first computer in Bangladesh was installed at the atomic energy centre, Dhaka of the then Pakistan Atomic Energy Commission in 1964. It was an IBM Mainframe Computer of 1620 series. The main use of the computer was resolving complicated mathematical calculations in different research works. Computer market becomes wider in the nineties. Greater acceptability of IT began in Bangladesh from the middle of the nineties. Information Technology is a well-known matter today.

In the sixties rapid expansion of bank and insurance as well as trade and commerce including scientific research at both home and abroad was increased. Rapidness in the job became necessary due to volume of routine accounting works. In many of the big organizations, maintenance of accounts manually became almost impossible. During

On the other hand Apple Computer Incorporate also released in the market Apple-Macintosh computer evolved by them. But the Apple did not adopt any liberal policy in making their compatible computer and hence the price of Macintosh computer remained very high that precluded it from achieving expected popularity. But due to some special practical privileges Apple-Macintosh were widely used particularly in printing industries.

PCs became easily available due to its easy use and cheapness in price. As a result, use of PCs started to increase in Bangladesh mainly since the last part of the eighties, especially in education and business concerns. From the mid-nineties computers are widely used in Bangladesh.

a. Innovation of Bangla software

In 1987, Bangla writing in computer was first materialized and an engineer namely Mainul Islam deserved the claim of this success. He managed to write Bangla in Apple-Macintosh computer using his self-evolved font 'Mainulipi'. The conventional English keyboard was used without using any separate keyboard for Bangla. The difference in type and form of Bangla and English alphabets and the problems relating to Bangla conjunct letters were solved using the advantage of four layer keyboard of Macintosh. Two more Bangla font, namely 'Shahidlipi' and 'Jabbarlipi' were evolved immediately after Mainulipi.

In 1988 the first Interface 'Bijoy' useable in Apple-Macintosh computer was built under the auspices of a non-government organization 'Anando Computers'. The layout of the first Bangla keyboard was also composed during this time. Among the initial keyboards, Bijoy and Munir are worth mentioning. In the Interface technique, the Bangla keyboard is attached with the Operating System (OS) of the computer and Bangla is inscribed in the computer by activating this keyboard and selecting a Bangla font. Bijoy, being a Macintosh based interface and the price of Apple-Macintosh computer being too high, number of its users was limited & confined to printing and publications.

The users of IBM computer were always more and keeping this in mind two higher secondary level students Reza-E Al Amin Abdullah (Aunko) and Md. Shahidul Islam (Sohel) evolved a self sufficient Bangla word processing software entitled 'Barna' in early 1992.

2001, the IT team of the National Encyclopedia of Bangladesh, Banglapedia, after much research, was able to attain success in sorting Bangla alphabets in computer.

The use of Bangla in computer, the role of computer in offices and printing industries in Dhaka rapidly assumed a great dimension. Exportable software development in Bangladesh commenced in 1995 while exportable multimedia system development began in 1997.

b. Use of Internet and e-mail

The use of Internet worldwide spread rapidly in 1990. Use of Internet in Bangladesh started in 1995 for the first time in a limited way through offline e-mail. VSAT (Very Small Aperture Terminal) was first set up in 1996 for Internet purpose. Online Internet connection started through an Internet Service Provider (ISP) named ISN. At present there are many ISPs in the country. Only BTTB (Bangladesh Telegraph and Telephone Board) is government owned ISP. Most of the ISPs are Dhaka based. Online Internet facilities are also available outside Dhaka in all District cities. The establishment of online Internet service a new horizon has been opened in the field of education, research, business and entertainment. With the expansion of online Internet facilities, various institutions and organizations have started to release their self-introductory WebPages. The official Web address of Bangladesh Government is www.banglagov.org where information regarding the country has been furnished in brief.

In the present ICT world E-mail is the cheapest, fastest and the most dependable media. Introduction of this system in Bangladesh become very popular and its use is increasing day by day right from individual level to all fields of education, office and commerce. With a view to introducing faster mail service Bangladesh Postal Department has arranged Electronic Post (e-post) at a number of post offices in the country. Under this postal system messages are sent and received through Internet. A good number of Cyber Cafes have been set up in Dhaka and other Cities where Internet facilities including web browsing are available.

Some educational institutions, training centers and business houses of the country started setting up Local Area Network (LAN) from the

Innovation of this independent word processor by these two meritorious programmers from their own firm 'Safeworks' was an epoch making event. This was DOS based (Disk Operating System), though the appearance of the programme was like the Windows. In the Barna, three types of keyboard could be used - Munir, Bijoy and Easy keyboard. The Barna also incorporated the advantage of keyboard restructuring (customise). That is, one could make out new keyboard layout according to one's liking or convenience.

Subsequently, with the introduction of better and better word processor versions in the market by Microsoft Corporation, an interface 'Bijoy' was evolved in 1993 with a view to using Bangla font and Bangla keyboard with Microsoft Windows in IBM computer. Later another interface namely 'Lekhani' was made available in 1994. 'Aabaha' (later part of 1992) was the first interface suitable for use in IBM computer. But its use remained restricted due to some lapses. Quite a few Bangla interfaces are prevalent at present, viz Bijoy, Lekhani, Proshika-Shabdo, Anirban, Barnamala, Prabartana, etc. Like more than one interfaces, a number of Bangla keyboards are also operating, viz Munir, Bijoy, National, Lekhani, Prabartana, ShahidLipi, etc.

Due to the absence of a universal keyboard layout in Bangla and the lack of harmony among different interfaces, a document composed by using a particular interface and keyboard layout can not be edited by using a different interface and keyboard layout. However converter programme is being attached in some interfaces recently or converter programmes are being compiled separately. A universal keyboard layout and proper coordination between different interfaces made by various companies are necessary to resolve this problem.

In keeping pace with interface and keyboard layouts Bangla font has also achieved sufficient development. Various fonts ranging from very common to artistic standard have been composed. Apart from word processor, Bangla keyboard and fonts can be used in various other application package programmes. For use with word processor different Bangla spell checking programmes have also been made, viz Pundit, Prashika Shabda-kosh, Lekhani, etc. But owing to the absence of any particular layout for Bangla font in the computer, no progress has been achieved so far in sorting Bangla alphabets in serial order. In

2001, the IT team of the National Encyclopedia of Bangladesh, Banglapedia, after much research, was able to attain success in sorting Bangla alphabets in computer.

The use of Bangla in computer, the role of computer in offices and printing industries in Dhaka rapidly assumed a great dimension. Exportable software development in Bangladesh commenced in 1995 while exportable multimedia system development began in 1997.

b. Use of Internet and e-mail

The use of Internet worldwide spread rapidly in 1990. Use of Internet in Bangladesh started in 1995 for the first time in a limited way through offline e-mail. VSAT (Very Small Aperture Terminal) was first set up in 1996 for Internet purpose. Online Internet connection started through an Internet Service Provider (ISP) named ISN. At present there are many ISPs in the country. Only BTTB (Bangladesh Telegraph and Telephone Board) is government owned ISP. Most of the ISPs are Dhaka based. Online Internet facilities are also available outside Dhaka in all District cities. The establishment of online Internet service a new horizon has been opened in the field of education, research, business and entertainment. With the expansion of online Internet facilities, various institutions and organizations have started to release their self-introductory WebPages. The official Web address of Bangladesh Government is www.banglagov.org where information regarding the country has been furnished in brief.

In the present ICT world E-mail is the cheapest, fastest and the most dependable media. Introduction of this system in Bangladesh become very popular and its use is increasing day by day right from individual level to all fields of education, office and commerce. With a view to introducing faster mail service Bangladesh Postal Department has arranged Electronic Post (e-post) at a number of post offices in the country. Under this postal system messages are sent and received through Internet. A good number of Cyber Cafes have been set up in Dhaka and other Cities where Internet facilities including web browsing are available.

Some educational institutions, training centers and business houses of the country started setting up Local Area Network (LAN) from the

phase of preservation, processing and analyzing of data collected from various surveys including formulation of database

In financial institutions including banks, particularly in private banks, maintenance of database and extension of various services are increasingly getting computer based. Computerization is also gradually under way in government banks. Foreign banks played a pioneering role in introducing computerized financial transactions in Bangladesh. By using ICT, banks are being able to give better services to their clients by establishing links with inter-branch, inter-bank as well as inter-continental banks. Most of the local private banks are following this today. Some local and foreign banks individually or collectively have been running Automatic Teller Machine (ATM) network by using ICT. ATM card device is fast spreading in the country's main cities. Credit card has also become popular all over the country since inception in 1999. Banks are going to online banking rapidly.

Various technology based departments and agencies of the Bangladesh Government viz SPARRSO (Space Research and Remote Sensing Organization), Bangladesh Meteorological Department, Survey of Bangladesh, Water Resources Planning Organization (WARPO), Geological Survey of Bangladesh, etc are using computer in formulation of their database and mapping. In particular, by using GIS (Geographical Information Systems) software, drawing of various types of skilful maps at shorter time is being possible. Bangladesh Meteorological Department is now able to provide faster and more accurate weather forecast by analyzing meteorological data collected from satellites and formulation of maps through computer. This is enabling people to take preparations during times of natural hazards and decreasing the volume of damages to much extent. Besides, analyses relating to weather and climatic changes are also being possible through computer modeling.

Bangladesh Election Commission has taken up a project to prepare a flawless voter list with the help of computer. Different government and non-government organizations are using Data Base Application Software to meet their respective requirements. Though this software were imported from abroad in the past, at present various local software companies are being engaged in most of the cases to make these customized software.

beginning of the 1990s. Among them Shahjalal University of Science and Technology, Rajshahi University and Bangladesh Open University have set up high standard optical fiber LAN backbone for internal communication. In 1997 a plan was undertaken to connect all the universities of the country through a Wide Area Network (WAN) called BURNET. Subsequently Dhaka University and BUET were brought under this network through radio link in 1999. Almost other universities have been brought under this network The government has another plan to connect the big libraries of the country through another Wide Area Network BANSLINK.

Bangladesh joined with Global Information through optical fiber Super Highway. Bangladesh's communication facilities with other countries of the world have established. With the establishment of this optical fiber cable link speed of Internet browsing increased manifold with decreasing cost and rates of international telephone calls are also expected to come down.

c. Computer assembling

No computer components are yet produced in Bangladesh. In most cases these are imported from China, Taiwan, Malaysia, Singapore and Korea. Besides, few computers and computer components are also imported from Japan, America and various European countries. Different local companies assemble most of the computers A few fully pre-assembled brand computers are also imported from abroad though their number is extremely limited. The government has made computer hardware, software and their accessories duty-free from 1998-99 fiscal years with a view to encourage the use and expansion of computer in the country. As a result, prices of computers in the country have decreased and their use multiplied many folds.

d. Use of computer

In Bangladesh today computer is being used in research and educational institutions, government and private organizations, business concerns including bank and insurance, industries, mills and factories, military installations almost every where. Among the government offices, Bangladesh Bureau of Statistics is the largest user of computers. The Statistical Bureau at present uses computer at every

phase of preservation, processing and analyzing of data collected from various surveys including formulation of database

In financial institutions including banks, particularly in private banks, maintenance of database and extension of various services are increasingly getting computer based. Computerization is also gradually under way in government banks. Foreign banks played a pioneering role in introducing computerized financial transactions in Bangladesh. By using ICT, banks are being able to give better services to their clients by establishing links with inter-branch, inter-bank as well as inter-continental banks. Most of the local private banks are following this today. Some local and foreign banks individually or collectively have been running Automatic Teller Machine (ATM) network by using ICT. ATM card device is fast spreading in the country's main cities. Credit card has also become popular all over the country since inception in 1999. Banks are going to online banking rapidly.

Various technology based departments and agencies of the Bangladesh Government viz SPARRSO (Space Research and Remote Sensing Organization), Bangladesh Meteorological Department, Survey of Bangladesh, Water Resources Planning Organization (WARPO), Geological Survey of Bangladesh, etc are using computer in formulation of their database and mapping. In particular, by using GIS (Geographical Information Systems) software, drawing of various types of skilful maps at shorter time is being possible. Bangladesh Meteorological Department is now able to provide faster and more accurate weather forecast by analyzing meteorological data collected from satellites and formulation of maps through computer. This is enabling people to take preparations during times of natural hazards and decreasing the volume of damages to much extent. Besides, analyses relating to weather and climatic changes are also being possible through computer modeling.

Bangladesh Election Commission has taken up a project to prepare a flawless voter list with the help of computer. Different government and non-government organizations are using Data Base Application Software to meet their respective requirements. Though this software were imported from abroad in the past, at present various local software companies are being engaged in most of the cases to make these customized software.

The management and running of large scale and important industrial concerns of the country are now much extent dependent on computer technology - particularly those industries where it is essentially important to keep intact the qualitative standard of the goods produced, for example, pharmaceutical industries. In these factories, qualitative standard of drugs is being ensured with the help of computer.

e. Computer organizations

In 1983 a national committee was formed aimed at purchasing computers to cater to the government requirements. In 1988 the committee was renamed as the National Computer Board. This Board was further reformed in 1989 and was made into an institution under the Ministry of Science and Technology in the name of Bangladesh Computer Council (BCC). BCC has now been working as a government advisory body on computer.

A number of professional bodies have been set up under non-government endeavors to steer ahead the computer-culture in the country. Of these, Bangladesh Computer Society is the pathfinder. The number of members of this Society, founded in 1979, is now well past four thousand. In 1992 computer businessmen set up Bangladesh Computer Samiti (BCS). Under the auspices of this association, an extensive computer market called BCS Computer City has been established at IDB building at Agargaon in Dhaka. BCS Computer Fair is organized every year in this Computer City. The Samiti also arranges regular computer fair in the country's main metropolis apart from Dhaka. There are a number of other computer professional bodies including Bangladesh Association of Software Industries and Services, ISP Association of Bangladesh etc.

f. Computer education

The institutional computer education began in Bangladesh in 1984 with the founding of the Computer Science and Engineering Department in BUET. The Computer Science Department at Dhaka University was established on 1st September 1992. At present departments for computer education have been opened in most government and non-government universities in the country as well as in four BITs (Bangladesh Institute of Technology). Computer Science

courses has also been opened at Honors level in a number of colleges affiliated with the National University. Computer education has been included in the syllabus at higher secondary level since 1991 and that of secondary level since 1994. Various private computer training centers have been playing vital role in disseminating computer literacy in the country since the middle of the 1990s. Many local computer training institutes are conducting training programmes jointly with various foreign universities and institutes.

At present quite a few computer related magazines are being published regularly. Some of these magazines also release Multimedia or CD (Compact Disk) versions side by side paper printed edition.

Programmes for establishing 'Computer and IT Villages' at Kaliakair in Gazipur district off Dhaka and at Mohakhali in Dhaka City have been taken at government initiative. Their use and culture of computer and information technology in Bangladesh increased many times.

[Ref. Masud Hasan Chowdhury,
Md. Mahbub Murshed and
Sifatul Quader Chowdhury]

2. Localization : Initiatives and Achievements

a. What is Localization of computer

Ability to use ICTs in the local language of the user is known as localization. Specifically, it is enabling computing experience in linguistic culture of the user. Bangla is the primary language for about 140 million people of Bangladesh. Organized effort of Bangla software development and content localization efforts are not very effective in the country. Before generation of any content or any application is developed, some basic standards for encoding the language must be developed. These include -

1. Character set encoding (ASCII/UNICODE),
2. Key board layout,
3. Key pad layout (e.g. for mobile telephones),
4. Collation sequence (to enable applications like database),

5. Terminology translation and locale definition (to enable computer interface in local language).

The first attempt of localization started in the early 1980s with Bangla font development in windows environment. Many fonts were developed in organized way resulting in a gross interoperability. There was no combined planned activity and policy in different key-board mapping and to make the localization process effective. In late 90's the UNICODE shed a new light on this issue. After that the process of localization began to take a new shape in this country. The open source software till then has the most significant affect in the localization. In 1998, Mr. Tanim Ahmed first solved the locale issue (bn.BD) and started a process of localization of Linux. Since then the major initiatives were run by the volunteers. In recent days the institutional initiatives are also appreciable.

Open content in Bangla language is rare in the Internet. Similarly, encyclopedic content in Bangla has traditionally been limited to the print media only. The Bangla Wikipedia provides a great opportunity to create an accessible, free, and constantly updated encyclopedia. Bangla, spoken about by 230 million people, is the 7th largest language in terms of native speakers. Therefore, it is vital to bridge the digital divide by introducing, expanding, and enhancing knowledge in Bangla language through the Internet.

b. Development of Localization in Bangladesh

In 1980s the windows based localization (Font / Interface) were lead by commercial vendors. In late 1990s with the appearance of Linux and open source software, voluntary communities were getting in. After the initial effort of Tanim Ahmed, more volunteers took steps into the localization effort. The voluntary group Ankur started localization of open source software like Linux, open office, gaim etc. The other voluntary organization Ekushey started developing open source, Unicode fonts and bangla input system. Some other volunteer groups and individuals came into scene. At this time the governmental efforts as well as any effective organizational efforts are not there. In 2004, Bangladesh Computer Council (BCC) took an initiative from the government site and came up with a national key board mapping and a collation sequence.

In this time, country's sole centre for localization has been created at BRAC University. The Center for Research on Bangla Language Processing (CRBLP) is currently conducting research projects that deal with Bangla language processing. At present the research team is working on Bangla information retrieval, (e.g., Bangla spell-checking, Bangla search engine), morphological analysis, developing a digital Bangla lexicon and an online dictionary, building an annotated Bangla corpus, Bangla computational syntax, Bangla optical character recognition and Bangla speech processing.

In 2005, Bangladesh Open Source Network (BdOSN) was formed with the local OSS volunteers. BdOSN, again a voluntary organization, took the Bangla localization as one of its main agenda and has started thriving OSS localization as the forerunner.

c. Achievement in OSS (Open Source Software) localization

Ankur and BdOSN completed the creation of glossary (Bangla term of computer term). Ankur and associates volunteers had already localized different Open Source Software (OSS). These included Linux distribution like Fedora, Mandriva, Suse and Ubuntu; Desktop environment like Gnome and KDE; Applications like OpenOffice.org, GAIM, Firefox and Thunderbird. All the above OSS needs are not completely localized. All these need a good intervention. For this BdOSN and Ankur started arranging Localization boot camp throughout the country since June 2006. Since then four boot camps were arranged and more than 10000 strings of Open office.org were translated in these camps. CRBLP developed an open source, full-featured cross-platform Unicode rich text editor capable of editing Bangla (BanglaPad), Bangla phonetic spelling checker and Java Interface for PC-Kimmo, a command line morphological analyzer provided by SIL. It was also noticed that in recent years more researches in the universities are now showing interest in localization.

d. What is Open content development

In Bangladesh, the main thrust sector in Open Content Development has been the development of the Bangla Wikipedia. It was organized by Bangladesh Open Source Network (OSN) and its sister organization, Bangla Wiki. The project aims at developing a free,

open access encyclopedia in Bangla language. Besides the Bangla Wikipedia, some initiatives have been started in recent years to develop some open content in science, especially in mathematics. The Bangla Wiki project aims at organizing contributors to the Bangla Wikipedia, publicizing it through print and electronic media, and providing the support infrastructure for collaboration.

e. Bangla Wikipedia development:

The Bangla Wiki project is loosely organized using Internet based mailing lists. Most of the participants are students in Bangladesh and West Bengal, or expatriates living in North America, Europe, and Japan. The organization has actively promoted Wikipedia and open content development activities in Bangladesh. It has conducted several workshops to familiarize the new users with techniques and skills related to the project. To promote public awareness, Bangla Wiki organized rallies during the Bangla New Year, and also observed August as the Bangla Wiki Month.

f. Future Localization development

In Bangladesh where a small portion of the majority communicates in English, it has become an absolute necessary to provide people the internet and other computing applications in Bangla. The initiatives have taken, proved to be fruitful. The Government has decided to post the Government websites in Bangla beside English and also many websites in Bangla only. Private organizations has also come a long way and are still moving on to make localization and open content development. The success of Bangla Wikipedia and the researches going on today are all proves of that. Hopefully, with this public private partnership, the localization and open content development in Bangladesh will be successful before not too long.

(Ref. Munir Hasan and Ragib Hasan)

QUESTION AND ANSWER ON THE INFORMATION AND COMMUNICATION ACT 2006

Chapter 1

1.1 Title of the Act:

The Information and Communication Act 2006

1.2 Objectives of the Act:

The objectives of the Act are to define and amend certain parts of law relating to legal recognition and security of Information and Communication Technology and related matters as follows:

1. To provide legal recognition for transactions related to electronic data interchange and the means of electronic communication and storage of information.
2. To facilitate Electronic filing of documents with the government Agencies, statutory corporations,
3. To amend Penal Code 1860, The Evidence Act 1872, and The Bankers Books Evidence Act 1891.
4. To minimise the incidence of forged electronic records, intentional and unintentional alteration electronic records, and fraud in e-commerce and other electronic transactions.
5. To establish uniformity of rules, regulations and standards relating to authentication and integrity of e-records.
6. To promote public confidence and practice of information and communication technology under a legal basis.
7. To establish the Cyber Tribunal and Cyber Appellate Tribunal.
8. To bring the conventional law and the Cyber law under the legal frame works.

1.3 Contents of the Act.

The Act contains total nine chapters and 90 sections. Under these nine chapters the following matters are discussed:

1. In chapter 1 the preliminary matters like title, definitions are discussed in Sections from 1 to 4.

2. In chapter 2 discussed about Digital Signature and Electronic Records from section 5 to 12.
3. In chapter 3 discussed about Attribution, Acknowledgement and Dispatch of Electronic records from section 13 to 15,
4. In chapter 4 discussed about secure electronic records and digital signature from section 15 to 17,
5. In chapter 5 discussed about Controller and Certifying Authority from section 18 to 40,
6. In chapter 6 discussed about duties of subscribers from section 41 to 44,
7. In chapter 7 discussed about penalties and adjudication from section 45 to 53,
8. In chapter 8 discussed about crime, investigation, judgement and punishment from section 54 to 84, and
9. In chapter 9 discussed about miscellaneous matters from section 85 to 90.

These are the brief idea about the contents of the Act.

1. 4 Characteristics of the Act.

The followings are the brief characteristics of the Act:

1. This Act comes from the legislative source of law,
2. This was the Act IXL of 2006.
3. It was passed by the Bangladesh parliament on 8 October 2006
4. It was extended to whole of Bangladesh,
5. It has come into force immediately, just after passing the Act.
6. Superiority of the Act on other prevailing laws or Acts.
7. The original Text is in Bengali and there is an English version. If there is any conflict between Bengali and English, Bengali text shall prevail.

1.5 Utility of the ICT Act 2006:

The ICT Act 2006 is an attempt to make a relation between the conventional laws prevailing at this time and to provide laws to find out ways to deal with cyber crime. In brief these are as follows:

1. Now days E-commerce is a tremendously growing industry and carries out business using information and communication technology. So it becomes essential to bring it in a legal frame work. The ICT Act 2006 is that legal frame work.

2. The ICT Act 2006 empowered the government to take necessary legal attempts to bring this very big industry under the control of the government and to make it comfortable and beneficial to the citizen for the betterment of the society and the civilization.
3. This Act facilitate the use of Digital signature with legal basis and to punish the unauthorized users for the benefit, reliability and authentication and the enforcement of the digital and E-transaction in the cyber space through computer net work.
4. This Act provides statutory remedy in case of crime committed by the accused and provide legal action against the accused by establishing the Cyber Tribunal and Cyber Appellate Tribunal in Bangladesh.
5. This Act also setup the territorial jurisdiction of cyber crime through cyber regulations and thus bring the ICT world under the legal frame work.

1.6 Purpose of the ICT Act 2006

The ICT Act 2006 is enabling to do the following task.

1. Legal reorganization of E-transecting and E-Record.
2. Legal reorganization of Digital Signature,
3. Recognize the E-communication,
4. Recognize the acceptance of E-contract,
5. Legalize the E-commerce, M-commerce, and Electronic data interchange,
6. Recognize the E-governance,
7. Recognize the Electronic filing of Documents, Retention of E-documents,
8. To bring uniformity in Rules, regulations, Authentication and Integrity of E-Records or E-Documents.
9. Authorise the publication of E-Gazette in E-form,
10. Transmission of message in encrypted of Electronic form,
11. To prevent Cyber Crime, local and international level.

1.7 The ICT Act 2006 and unauthorized Access:

Unauthorized access to any computer or any computer system is an offence. This is discussed in the ICT Act 2006 under section 54. According to this section, If any person without permission of the

owner or any other person who is in charge of a computer, computer system or computer network;

1. access or secure access to such computer, computer system or computer network;
2. Downloads, copies, or extracts any data, computer data base, or information from such computer, computer system or computer network;
3. Introduce or causes to be introduced any computer, computer system or computer network;
4. Damage, causes to be damaged any computer, computer system or computer network;
5. Disrupts or causes disruption of any computer, computer system or computer network by any means;
6. Provide any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, or rules or regulations made; thereunder.
7. Change the services availed of by a person to the account of another person by tempering with or manipulating any computer, computer system or computer network;

This person shall be liable to pay compensation to the affected person not exceeding Taka 1 crore.

1.8 Provision for discloser of confidentiality and privacy:

Brach of privacy is an offence. and is rewarded punishment under section 63 of this Act, which protect the constitutional agreement through Article 43 of the Bangladesh Constitution and stated as follows:

Every citizen shall have the right, subject to any reasonable restriction s imposed by law in the interest of the security of the state, public order, public morality or public health-

1. To be secured in his home against entry, search and seizure and
2. To the privacy of his correspondence and other means of communication.

Section 63 of the ICT Act 2006 ensures the privacy from another person as follows:

Save as otherwise provided by this Act or any other law for the time being is force, no person who in pursuance of any of the powers

conferred under this Act or rules, and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document, or other material shall without the consent of the person concerned, discloser of such electronic record, book, register, correspondence, information, document, or other material to any other person.

1.9 Weaknesses of the ICT Act 2006

The ICT Act 2006 is a brilliant achievement of Bangladesh in the legal field of Cyber law. This law regulates and controls the information technology of Bangladesh. The government stated that thee is nothing new in enacting such law as similar provisions already exist in other statutes. There are sufficient safeguards in the ICT Act itself which provides the provision to apply the Code of Criminal Procedure if required for the trial of the cyber offence.

The ICT Act 2006 appears to be self sufficient to deal with all cyber crime and to protect the emergent IT industry. But still there are some weaknesses. These are as follows:

1. Intellectual property rights are an important issue in the legal field. But this Act remain silent about the provisions of copy right, trade mark, and patent right of e-information and data. This law does not take any rights and liabilities of domain holders of e-commerce, m-commerce etc.
2. Electronic payment is a negotiable instrument from the point of applicability of IT Act. It has a major effect e-commerce, m-commerce in Bangladesh. But the ICT Act 2006 remains silent in this respect.
3. Internet is a borderless entity and has an international implication. Cyber crime has no specific territorial jurisdiction. But this Act has no clear direction regarding these jurisdictional problems and enforcement of law in the international perspective.
4. Cyber defamation is very important issue. Transmission of defamatory substance is a offence. Though defamation is punishable under section 500, 5001 and 5002 of the penal code 1860. But this is not sufficient is context of cyber defamation.
5. Deputy Superintendent of Police is empowered to investigate and to file charge sheet related to cyber crime and cyber law. This approach is likely to be misuse in the context of

Bangladesh. The companies relating to IT have public offices which would come within the ambit of public place under this act. As a result companies may be the victim of potential harassment of official complexity.

Beside these weaknesses there are some other limitations of this Act, which will come in day light during the time of implementations. In spite of these weaknesses the ICT Act 2006 is a good law for IT sector in the implementation of Cyber law to protect Cyber crime.

Chapter 2

2.1 Electronic Signature:

Electronic Signature authenticates the identity of the sender. It ensures the original contents of the message remain unchanged. It is easily transferable. It can not be easily repudiated and can nor be imitated. An electronic is a computer data compilation of any symbol or symbols. They are the electronic equivalent to hand written signature on paper. It is based on biometric identification method or facial and voice recognition. It is a simple combination of ID and password. The user ID must be unique to a specific person.

The ICT Act 2006 allows a person to satisfy legal requirements for a manual signature. An electronic communication is a method that identifies the person and indicates that approval of the information

communicated. The method by which a person is identified electronically is commonly called 'electronic signature'. The choice of a particular method must be a reliable as appropriate in the circumstances. The legislation provides flexibility to the people to determine the signature technology to their particular need. The method is not a unique identifier.

2.2 Digital Signature:

Digital signature is an important issue in the field of IT to make e-contract. It is an encrypted form of files relating to e-message, e-documents, e-programme etc. Encrypt means converting ordinary language into code. It is a new technology to safeguard the interest of the parties in e-contract during the e-transaction. To forge Digital Signature is mare impossible. Digital signature comes from a digest of the text encryption and send with the text message. The recipient decrypts the signature and retrieves the digest from the received text. Decrypt means converting code into ordinary language. Digital signature is required for open systems for higher security levels. Digital signature is always implementing electronic signature. It refers to any electronic data that carries the intent if the signature. But all electronic signatures does not use digital signature.

2.2.1 Definition of Digital Signature:

The section 2(1) of the ICT Act 2006 defines Digital Signature that, "Digital signature" means any data in electronic form that (a) Is attached with some other electronic data reasonably; and (b) Any justification of any digital signature will be done subject to the following conditions- (i) That is attached with the signer similarly. (ii) That is able to recognize the signer. (iii) That is created through such a secure method that can confirm the signer's control. (iv) That is attached to the data in such a way that it can recognize any change in the very data.

2.2.2 Characteristics of Digital Signature:

1. Digital Signature is required for open system
2. It ensures the higher security level in e-transaction.
3. A digital signature is an electronic signature.
4. It based on cryptographic methods of originator authentication.
5. It is computed by using a set of rules and a set of parameters.
6. These are the identity of the signer and the identity of the data to be verified.

7. In the case of e-commerce digital signatures are especially important. It is a key component of most authentication schemes.
8. Digital signature is not forgeable. There are several encryption techniques to guarantee the level of security.
9. Like a written signature the individual message sender can really on a digital signature.

2.2.3 Classification of Digital Signature:

There are 3 classes digital signature:

1. This class of digital certificate does not hold any legal validity. In this case the verification process is based only on a valid e-mail ID and involves no direct verification.
2. This class states that a person's identity is to be verified against a trusted, pre-verified database.
3. This class requires the person present himself in front of a Registration Authentication (RA) and prove his/her identity.

2.2.4 The digital certificate contains the followings data:

(a) Owner's name and address;
(b) Company's Name and address
(c) Owners public Key, along with certificate's serial number and validity period. and
(d) Certifying Company's ID and its digital signature.

2.2.5 Functions can be done electronically:

(1) The credit investigation,
(2) Loan processing,
(3) Underwriting documents,
(4) Documents preparation.

The borrower can sign

(1) All loan papers,
(2) The mortgage deeds,
(3) The trust deeds, and
(4) Notarized

over the internet.

2.3 Meaning of the following terms:

2.3.1 Electronic Record

2.3.2 Retention of Electronic Records,
2.3.3 Electronic Gazette,
2.3.4 Online Contracts,
2.3.5 Electronic Records and digital signature in Government office
2.3.6 Liabilities of Documents in Electronic Form.

2.3.1 Electronic Record:

The records which are communicated and maintained through electronic equipments are known as electronic records. It is the combination of text, graphics, data, audit, pictorial or other information representation in digital form. It may be created, modified, maintained, archived, retrieved or distributed by a computer system and can be stored on an electronic storage media and it may only retrievable through electronic means.

Section 2(7) of the ICT Act, 2006 defined that 'Electronic Record' means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche. For purpose of this definition 'electronic record' does not include or refer to photocopies, digital imaging systems or analog or digital audio and video tapes

2.3.2 Retention of Electronic Records:

Retention literally means the act of keeping in possession something. So the retention of electronic record is an act of retaining computer based records in digital storage media. This is for specific period of times corresponding in size or degree or extent with their value. The disposal or permanent preservation is concern with the official organizational policy. Electronic records retention program is that portion of the organization's that provides policy and procedures specifying the length of time that computer-based records must be maintained.

The ICT Act 2006, section 9 has provides rules regarding Retention of electronic records. These are as follows:

(1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:-

(a) The information contained therein remains accessible so as to be usable for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) A person may satisfy the requirements referred to in sub -section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

(3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records.

2.3.3 Electronic Gazette:

Gazette is a newspaper or official journal generally published by the Government. So, Electronic Gazette is a newspaper or official journal generally published by the Government through electronic media. Section 10 of the ICT Act 2006 has given the recognition of Electronic Gazette as follows:

Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye- law, notification or any other matter is published in the Official Gazette or the Electronic Gazette:

Provided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

2.3.4 Online Contracts:

Online means that computer connected to another computer through a computer network or accessible by computer. So Online

Contract means a contract which is perform by using computer network. Now day most of the business contract are made through online. For example a business man makes a sale contract with another business man of another country; open Letter of credit (L/C) etc is a common practice of online contract.

E-commerce has specified detailed transaction rules. A contract concluded under this rule over the internet is online contract. The ICT Act 2006 has provides legal recognition and protects the electronic records and digital signature.

Section 2(7) of the ICT Act, 2006 defined that 'Electronic Record' means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche. For purpose of this definition 'electronic record' does not include or refer to photocopies, digital imaging systems or analog or digital audio and video tapes.

Section 6 of The ICT Act 2006 has given Legal recognition of electronic records as follows: "Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form then notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form: Provided that the information or any matter shall be accessible so as to be usable for a subsequent reference."

Section 7 of The ICT Act 2006 has given Legal recognition of digital signatures as follows: Information or any matter shall be authenticated by affixing the signature; or Any document shall be signed or bear the signature of any person; notwithstanding anything contain in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

The ICT Act 2006 has provides evidential value of electronic records. For this section 65 of Evidence Act duly amended. Under these circumstances the online contract is save and secure in Bangladesh.

2.3.5 Electronic Records and digital signature in Government office:

The ICT Act 2006 has given legal recognition to use Electronic Records and digital signature in Government office. In this regards section 8 of the ICT Act 2006 provides the following provisions:

(a) The filing of any form, application or any other document with any office, body, authority or agency owned or controlled by the Government in a particular manner;

(b) The issue or grant of any licence, permit, sanction, approval or order by whatever name called in a particular manner;

(c) The receipt or payment of money in a particular manner,

Then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing issue, grant, receipt or payment, as the case may be, is affected by means of such electronic form as may be prescribed by the Government.

So the Government may, for the purposes of sub- section (1) of this section, by rules, prescribe the manner and format in which such electronic records shall be filed, created or issued; the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record.

2.3.6 Liabilities of Documents in Electronic Form:

Relative provisions has provided under section 11 of the ICT Act 2006 as follows Nothing contained in this Act shall confer a right upon any person to insist that any Ministry or department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Chapter III

Attribution, Acknowledgement and Despatch of Electronic Record

3.1 Attribution of Electronic Record:

3.2 Acknowledge of receipt of Electronic Records:

3.3 Time and Despatch of Electronic Records:

3.1 Attribution of Electronic Record:

Electronic record is a faceless transaction between the strangers. In an electronic environment it is difficult to ascertain who the originator of electronic records is. The Originator is the person that the recipient believes him as originator. The attribution of the electronic record applies among the parties. Generally the originator or the sender of the electronic record is bound by that electronic record. An originator can refuse to acknowledge an electronic record once it has sent and not be hold responsible for any reliance on such a record by the recipient. If a security procedure is used then its attribution may be established and can be shown.

The provisions of attribution has described in section 13 of the ICT Act 2006. According to this section the provisions are as follows:

1. 1. An electronic record shall be attributed to the originator if by the originator himself or sent by a person who had the authority to act on be half of the originator.
2. As between the originator and the addressee, an electronic record shall be deemed to be that of the originator if it was sent-

(a) By a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(b) By an information system programmed by or on behalf of the originator to operate automatically.

3. As between the originator and the addressee, an addressee shall be entitled to regard an electronic record as being that of the originator and to act on that assumption.
4. Sub-section (3) of this section shall not apply-

(a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

(b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using reasonable care or using any agreed procedure, that the electronic record was not that of the originator; or

(c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

5. Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator or the addressee is entitled to act on the assumption, then, as between the originator and the addressee, the addressee shall be entitled to regard the electronic record received as being what the originator intended .o send and tp act on that assumption:
6. Whatever is stated in section (5) the addressee shall not be so entitled when the addressee knew or should have known, after exercising reasonable care or using any agreed procedure that the transmission resulted in any error in the electronic record as received.
7. The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption. But this will not be applicable on the following records,

   (a) If the addressee duplicate another electronic record or

   (b) If addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate.

3.2 Acknowledge of receipt of Electronic Records:

Generally electronic records require acknowledgement from the recipients. Acknowledgement of receipt of electronic records among the parties is requiring in electronic transaction. The originators of electronic records intended acknowledgement from the recipient.

If the method of acknowledgement has not been agreed to by the parties involved in the electronic transaction, in that case any method of acknowledgement may be used and it will be sufficient to be considered as receipt.

If an electronic record is conditional on receipt of acknowledgement and the transaction if not followed the conditional method, then the transaction will be treated as if it were never sent.

In case the electronic record is not stated conditional on receipt of acknowledgement, an originator may subsequently impose this condition and specify a time frame in which acknowledgement must be received. If not received in that time frame and it will be treated the original transaction as never sent.

Regarding the acknowledgement of receipt of electronic records the legal provisions has been described if section 14 of the ICT Act 2006 as follows:

Acknowledgement of receipt.-

(1) Sub- sections (2) (3) and (4) of this section shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –

(a) Any communication by the addressee, automated or otherwise; or

(b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stipulated that the electronic record shall be conditional on receipt of the acknowledgement, then, until the acknowledgement has been received, the electronic record shall be deemed to have been never sent by the originator.

(4) Where the originator has not stipulated that the electronic record shall be conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator-

(a) May give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) If no acknowledgement is received within the time specified in clause (a) of this sub-section, may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

(5) Where the originator receives the addressee's acknowledgement of receipt, it shall be presumed that the related electronic record was received by the addressee, but that presumption shall not imply that the content of the electronic record corresponds to the content of the record received.

(6) Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it shall be presumed that those requirements have been met.

3.3 Time and Despatch of Electronic Records:

In case of legal transaction time determination is required at which notification is considered to have been given or received. Regarding these provisions has been described in section 15 of the ICT Act 2006 as follows:

Time and place of dispatch and receipt of electronic record.-

(1) When the originator and the addressee not agreed otherwise-

(a) The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(b) The time of receipt of an electronic record shall be determined as follows, namely-

(I) If the addressee has designated a computer resource for the purpose of receiving electronic records, receipt occurs,-

(i) At the time when the electronic record enters the designated computer resource; or

(ii) If the electronic record is sent to a computer resource of the addressee that is not designated computer resource, at the time when the electronic record is retrieved by the addressee;

(II) If the addressee has not designated a computer resource along with specified timing, if any, receipt occurs when the electronic record enters the computer resource of the addressee,

(c) An electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(2) Though the provisions of sub-section 1(c) regarding electronic device or system or the place of source of computer is different from sub-section 1(b), the later one shall apply.

(3) For the purpose of this section,-

(a) If the originator or the addressee has more than one place of business, the principle place of business shall be the place of business;

(b) If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

Explanation: in case of any registered organization 'the principal place of business" or "usual place of residence" means the place where it is registered.

Chapter IV

Secure Electronic Records & Secure Digital Signatures

4.1 Secure Electronic Records:

4.2 Secure Digital Signatures:

4.1 Secure Electronic Records:

An Electronic Records must qualify as a secure Electronic Records in a normal technological manner. To secure Electronic Records should be verified through

(1) A qualified security procedure,

(2) Commercially reasonable under the circumstances,

(3) Implemented in a trustworthy manner, and

(4) Relied upon reasonable and in good faith.

Legal provisions are described in section 16 of the ICT Act 2006 as follows:

Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

4.2 Secure Digital Signatures:

An Electronic Signatures must qualify as a secure Electronic Signature in a natural technological manner. To secure Electronic Records should be verified through. Legal provisions are described in section 17 of the ICT Act 2006 as follows:

Secure digital signature:

(1) If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

(a) Unique to the person affixing it;

(b) Capable of identifying the person affixing it;

(c) Created in a manner or using a means under the sole control of the person affixing it'

Then such electronic signature shall be deemed to be a secure electronic signature subject to sub-section (2), of the Act.

(2) Though the provision of sub-section (1), the electronic signature would be invalidated, the electronic record was altered.

Chapter V

Controller & Certifying Authorities

5.1 Controller, Sub-Controller, Assistant Controller

Section 2(21) defines "Controller" or "sub-controller" or "assistant Controller" means the "Controller" or "sub-controller" or "assistant Controller" of Certifying Authorities appointed under sub-section (1) of section 18 of this Act;

5.1.1 Appointment:

Controller, Sub-Controller, and Assistant Controller are appointed as per provisions of Section 18(1) of the Act, that, "The Government may, for the purpose of fulfilling the aim of the Act, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act, within 90 days of the date of passing of the Act.. The Government may, by notification in the Official Gazette, also appoint such number of Deputy Controllers and Assistant Controllers it deem fit.

So appointment of Controller, Sub-Controller, and Assistant Controller are appointed are under the control of the Government. They are to be appointed within 90 days from the passing of this Act. The notice of the appointment is to be published in the official gazette.

1.2 Functions of the Controller of Certifying Authority:

The functions of the Controller of Certifying Authority are to regulate and to control operation of Certifying Authority under section 18 of the Act. The duty of the Controller of Certifying Authority includes licensing, certifying, monitoring, and observing the activities of all certification authorities in Bangladesh under section 19 of the ICT Act 2006. According to section 19, (1) the Controller may perform all or any of the following functions, namely:-

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys of the Certifying Authorities;

(c) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(d) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(e) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certifying and the public key;

(f) Specifying the form and content of a Electronic Signature Certificate and the key;

(g) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(h) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them

(i) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(j) Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(k) Resolving any conflict of interests between the Certifying Auhorities and the subscribers;

(l) Laying down the duties and responsibilities of the Certifying Authorities;

(m) Resolving the computerized data that can: (i) Maintaining database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, (ii) Be accessible to the members of the public.

(n) Performing those works laid by this works or any work laid by any other Act.

(2) The Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.

(3) The Deputy Controllers and the Assistant Controllers shall perform such functions as are assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Government.

(5) The Head Office of the Controller shall be in Dhaka and Branch Offices of the office of the Controller shall be at such places as the Government may specify and may be established at such places as the Government may think fit for any specific time decided by the Government.

(6) There shall be a seal of the office of the Controller as the Government may specify.

(7) Under this Act, there shall be a room for reserving all electronic record in the controller's office and these rooms shall be called "electronic reservation room".

5.1.3 Power of the Controller of Certifying Authority:

The power of the Controller of Certifying Authority include are described in The ICT Act 2006 which are as follows:

1. Power to delegate: According to section 28 the Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any other officer to exercise any of the powers of the Controller under this Chapter.

2. Power to investigate: According to Section 29

The Controller or any officer, authorised by him

1. May investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

2. Have the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908, when trying a suit in respect of the following matters, namely:-

(a) Discovery and inspection;

(b) Enforcing the attendance of any person and examining him on oath or affirmation;

(c) Compelling the production of any documents; and

(d) Issuing commissions for the examination of witness.

3. Access to computers and data: According to Section 30,

1. Without prejudice to the provisions of section 45 of this Act, if the Controller has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made thereunder has been committed, he has the power to access any computer system, apparatus, data or any other material connected with such system, for obtaining any information or data contained in or available to such computer system.

2. For the purpose of sub -section (1) of this section, the Controller may direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

4. Power of controller to order in emergency time: According to Section 46,

1. If the Controller is satisfied on the grounds that there are necessary to give any order for practicing the sovereignty, unity, security of Bangladesh, the relationship with the other countries and public welfare of the country or for the purpose of controlling any crime under this Act, the controller may give order to any law enforcing authority for restricting of telecasting any data with the help of any computer system provided that the reasons behind the order should be written on the order form.

5. Power to announce any reserved system: According to Section 47,

1. The Controller may with the authority of the Government or willingly using the electronic gazette, declare any computer, computer system or computer network as the reserved system.

2. For the purpose sub-section (1), for securing the declared reserved system, the controller with written order may give a person the authority to do the work.

6. Controller to act as repository:

The Controller may act as the Repository (means a person to whom a secret is entrusted) of all Digital Signature Certificate issued under this Act.. According to Section 21,

1. The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

2. The Controller shall ensure that the secrecy and security of the digital signatures are assured and in order to do so he shall make use of hardware, software and procedures that are secure from misuse and observe such other standards as may be prescribed by the Government.

5.2 Certifying Authority:

The section 2(33) define "Certifying Authority" means a person who has been granted a license under section 22 of this Act to issue a Digital Signature Certificate.

A "Certifying Authority" is a trusted third party who can verify the identity of an applicant registering for a digital certificate. If he is satisfied about the authenticity of an applicant's identity, he may issue a digital certificate binding his or her identity to a public key. The Controller of Certifying Authority will appoint Safe Script as the first Certifying Authority in Bangladesh.

5.2.1 36. Issue of certificate:

According to section 36

(1) The Certifying Authority may issue a certificate to a prospective subscriber only after the Certifying Authority.

(a) Has received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber; and

(b) Has a certificate practice statement, complied with all the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber;

(c) Has confirmed by itself or through as authorised agent that the prospective subscriber is the person to be listed in the certificate to be issued;

(d) Has the confirmation of the information in the certificate to be issued is accurate: the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) Has been paid such fees prescribed for issuance of certificate.

5.2.2 Assurance by certifying authority:

According to section 37

(1) By issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement under sub-section (1) of this section, the certifying Authority represents that it has confirmed that –

(a) the Certifying Authority has complied with all applicable requirements of this Act and the rules and regulations made thereunder in issuing the certificate, and if the Certifying Authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(b) All information in the certificate is accurate, unless the Certifying Authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(c) The Certifying Authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in clauses (a) to (b) of this subsection.

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, sub -section (2) of this section shall apply to the extent that the representations are not inconsistent with the certification practice statement.

5.3 Electronic Record Reservation Room:

According to section 18(7) there shall be a room for reserving all electronic record in the controller's office and these rooms shall be called "electronic reservation room".

5.4 Validity of Digital Signature Certificate issued by Foreign Certifying Authority:

The Controller of Certifying Authority may give recognition to the Digital Signature Certificate issued by Foreign Certifying Authority as provisions of the section 20 of this Act and that will be valid.

According to section 20(1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

2. Where any Certifying Authority is recognised under sub- section (1) of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

3. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub -section (1) of this section, he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

5.5 Digital Signature Certificate:

Section 2(2) defines "Digital Signature Certificate" (DSC) means a certificate issued under section 36 of this Act. A Digital Signature Certificate can be presented electronically to prove the user's identity, to access information or service on the internet or to sign certain documents digitally. Electronic documents are required to be signed digitally through Digital Signature Certificate. A Certifying Authority may issue a Digital Signature Certificate under section22 of the ICT Act 2006 and it will become valid for Bangladesh.

5.5.1 Revocation of Digital Signature Certificate:

According to section 38

(1) A Certifying Authority shall revoke a Digital Signature Certificate issued by it on the following grounds.

(a) Where the subscriber or any person authorised by him makes a request to that effect; or

(b) Upon the death o f the subscriber;

(c) Where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub -section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that -

(a) A material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) A requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) The Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) The subscriber has been declared insolvent by a competent court or authority.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

5.5.2 39. Suspension of Digital Signature Certificate-

According to section 39

(1) Subject to the provisions of sub -section (2) of this section, the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate under the following grounds.

(a) On receipt of a request to that effect from the subscriber listed in the Digital Signature Certificate; or Any person duly authorised to act on behalf of that subscriber;

(b) If it is of opinion that the Digital Signature Certificate should be suspended in public interest by the certifying authority.

(2) A Digital Signature Certificate shall not be suspended under sub-section 1(b) without giving a notice of 30 days to the concerned authority.

(3) As an effect of the measure taken by the authority, under sub-section 2 of the section, if the Certifying Authority is not satisfied with the response of the subscriber, the authority can suspect the license. .

(4) The Certifying Authority may inform the subscriber after suspending such Digital Signature Certificate.

5.6 License:

Section 2(31) of the ICT Act 2006 define "Licence" means a licence granted to a Certifying Authority under section 22 of this Act. According to the provision this Act a Certifying Authority may provide a license in favour of a person to issue Digital Signature Certificate. So license is an important instrument in respect of Digital Signature Certificate. The license is transferable and revocable.

5.6.1 Application for license:

For the issuance of a license an applicant should apply for a license in a prescribed form to the government according to the provisions of section 23 of ICT Act 2006. The application should accompany with the followings:

1. A certification practice statement,
2. A statement including the procedures with respect to identification of the applicant.
3. Proof papers of payment of various fees,
4. Such other documents as may be prescribed by the government,
5. The license should be renewed annually for a prescribed period by paying fixed price (Section 24)

5.6.2 Grant or rejection of license:

As per provisions of section 22 of the ICT Act 2006, the Controller may grant a license or reject an application after considering the documents accompanying the application and other factors as he deem fit. The applicant has been given reasonable opportunity to present his case before rejecting the application.

5.6.3 Revocation and suspension of License:

According to section 26 of the ICT Act 2006, the Controller may stop or nullify any license if he is satisfied after making inquiry that the Certifying Authority has-

1. Made an incorrect or false statement in material particulars in relation to the application to issue or renewal of license,
2. Failed to comply with the terms and conditions to which the license was granted.
3. Failed to maintained the standards specified under section 21 (2)(b) of this Act.
4. Contravened any provisions of this Act, rules, regulations or orders made hereunder.

a. No license can be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation. Sec-26(2)

b. If the Controller may has reasonable cause to believe that there is any ground for revoking a license by order, suspend such license pending the completion of any enquiry ordered by him. Sec- 26(3)

c. Where the license of a Certifying Authority is revoked or suspended, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him.

d. No license shall be suspended for a period exceeding fourteen days unless the certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension. Sec- 26(4)

e. A Certifying Authority whose licence has been suspended shall not issue any Electronic Signature Certificate during the period of such suspension. Sec- 26(5)

f. (1) Where the license of a Certifying Authority is revoked or suspended, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him. Sec-27(1).

g. Where one or more repositories are specified, the Controller shall publish notices of such revocation or suspension, as the case may be, in all such repositories: Sec-27(2)

5.6.4 Display of license:

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carriers on its business. Sec-33.

Criticism: This section may be mistake and needs modification. The office of the Certifying Authority is not the proper place to visit physically. Foreign Certifying Authority may not have their office in Bangladesh. These provisions may be problem for them. This may be considered.

5.6.4 Surrender of license:

Every Certifying Authority whose license is revoked or suspended shall immediately after such revocation or suspension, surrender the license to the Controller. If he is failed to surrender shall be guilty of an offence under section 58 and shall be punished with imprisonment of either description for a term which may extended to six months or with fine which may be extended to taka ten thousand or with both.

Chapter VI

Duties of Subscribers

6.1 Duties of Subscribers:

6.1.1 Applying the security procedure:

6.1.2 Acceptance of Digital Signature Certificate:

6.1.3 Obtaining Digital Signature Certificate.

6.1.4 Control of private key:

6.1 Duties of Subscribers:

Section 2(15) define "Subscriber" means a person in whose name the Digital Signature Certificate is issued. So subscribers should have duties. According to the provisions of the ICT Act 2006 the duties of the Subscribers are as follows:

6.1.1 Applying the security procedure:

According to section 41 of the ICT Act 2006,

Where any Digital Signature Certificate the public key of which corresponds to the private key of their subscriber which is to be listed in the Digital Signature Certificate has been accepted by the subscriber, the subscriber shall generate that key pair applying the security procedure.

6.1.2 Acceptance of Digital Signature Certificate:

According to section 42 of the ICT Act 2006,

1. A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate to one or more persons; or in a repository; or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

2. By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

(a) All representations made by the subscriber to the Certifying Authority and all materials relevant to the information contained in the Digital Signature Certificate are true; and

(b) All information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

6.1.3 Obtaining Digital Signature Certificate.

According to section 43 of the ICT Act 2006,

All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

6.1.4 Control of private key:

According to section 44 of the ICT Act 2006,

1. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

2. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in such manner as may be specified by regulations.

Chapter VII

Penalties and Adjudication

7.1 Penalties and Adjudication

7.2 Penalty for Failure to Furnish Document, Return or Report:

7.3 Penalty for failure to file return, information, books:

7.4 Penalty for Failure to Maintain Books of Accounts or Records:

7.5 Residuary penalty

7.6 Fine for Infringement of Rules or Regulations of ICT Act:

7.1 Penalties and Adjudication

There are provisions for penalties and adjudication in Bangladesh Information and Communication Technology Act, 2006. The provisions are laid down in chapter 7. The Act has the provisions for appointment of an officer not below the rank of a Director to the Government of Bangladesh or an equivalent officer of Government as an adjudicating officer. The adjudication officer has given the power of a civil court.

7.2 Penalty for Failure to Furnish Document, Return or Report:

According to section 48 of the ICT Act 2006,

Whoever fails to furnish any document, return or report to the Controller or the Certifying Authority which he is required under this Act, or rules or regulations made thereunder to furnish shall be liable to pay a penalty which may extend to Taka two lakh for each such failure.

7.3 Penalty for failure to file return, information, books:

According to section 49 of the ICT Act 2006,

Whoever fails to file any return or furnish any information, books or other documents within the time specified therefore in this Act, or rules or regulations made thereunder the controller or any person authorised by the government may give an order to pay a penalty which may extended to take ten thousand for every day during which such failure continues.

7.4 Penalty for Failure to Maintain Books of Accounts or Records:

According to section 50 of the ICT Act 2006,

Whoever fails to maintain books of account or records which he is required under this Act, or rules or regulations made thereunder, the controller or any person authorised by the government may give an order to pay a penalty which may extended to Taka two lack.

7.5 Residuary penalty

According to section 51 of the ICT Act 2006,

Whoever contravenes any rules or regulation made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay compensation, made in a written form provided with reasonable grounds behind the penalty, the penalty not exceeding Taka twenty five thousand by such contravention, by the controller or any person authorised by the government.

7.6 Fine for Infringement of Rules or Regulations of ICT Act:

According to section 53 of the ICT Act 2006,

1. In addition to the fine mentioned under this Act, the controller may impose fine for infringement of rules or regulations made there under.

2. Any fine under this Act cannot be made by the controller to any person without giving him the chance of hearing with reasonable hearing.

3. Within seven days of giving fine to a person by the controller, the aggrieved person may apply to the controller for re-considering the fine given and the controller within 15 days will settle the matter by giving the aggrieved person a reasonable opportunity of hearing.

4. If fine made under this Act is not paid then it will be considered Actionable as government deemed under Public Demand Recovery Act 1913 (Bengal Act III of 1913).

Chapter VIII

Crime Investigation, Judgement and Punishment

Part 1

Crime and Punishment

8.1 Introduction:

8.1.1 Civil offence; Under Section 54 of the ICT Act 2006

8.1.2 Criminal offence; Under Section 54 to 67 of the ICT Act 2006

8.2 Damage to computer and Computer System and Penalty:

8.3 Hacking with Computer System:

8.4 Online Pornography in Bangladesh:

8.1 Introduction:

This Chapter discussed about Cyber crime, investigation, judgment and punishment. This chapter divided into three parts. Part 1 discusses about crime and punishment, Part 2 discusses about establishment of Cyber Tribunal and Part 3 discuss about the Cyber appeal Tribunal. This Chapter contains section 54 to 84. This Act deals in both civil offence and Criminal offence. These are describing here.

8.1.1 Civil offence; Under Section 54 of the ICT Act 2006

1. Unauthorised accesses to computer, computer system or computer network.

2. Unauthorised downloads, copies or extracts any data, computer database or information,

3. Introduce or causes to be introduced any computer virus,

4. Disruption of computer, computer system or computer network;

5. Denial of access to any person authorised to access any computer,

6. Provide assistance to any person to facilitate unauthorised access to a computer,

7. Changing the services availed of by a person to an account of another person by tempering with or manipulating any computer,

8.1.2 Criminal offence; Under Section 54 to 67 of the ICT Act 2006

1. Damage of computer, computer system or Computer network.[Sec-54(d)]
2. Tampering with Computer source documents, .[Sec-55(1)]
3. Hacking with Computer system, .[Sec-56]
4. Publication of obscene information in electronic form, .[Sec-57]
5. Failure to surrender license .[Sec-58]
6. Failure to comply with order of controller .[Sec-59]
7. Violation of controller's order in emergency time, .[Sec-60]
8. Unauthorised access to protected computer, .[Sec-61]
9. False representation and hiding information .[Sec-62]
10. Breach of Confidentiality and privacy .[Sec-63]
11. Publication of digital signature certificate for false and fraudulent purpose, .[Sec-64, 65]
12. Using Computer for committing an offence .[Sec-66]
13. Offence and contravention by companies, .[Sec-67]

8.2 Damage to computer and Computer System and Penalty:

Damage to computer and computer system is one of the cyber crimes and this crime is liable to be punished. Section 54 of ICT Act 2006 discusses about this as follows:

Damage to Computer and computer includes Section 54(1)

The act of a person shall be considered to be a crime under this Act. if he-

(a) Accesses or secures access to such computer, computer system or computer network for the purpose of having data or destroy it;

(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) Introduce or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damage or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any such computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised 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, or rules and regulations made there under;

(h) Willingly without the permission of the receiver or the sender, to advertise any service or commodities, produce or make marketing of span or try to do it or send mails unnecessarily;

(i) Change the services availed of by a person to the account of another person by tempering with or manipulating any computer, computer system or computer network;

Penalty for this crime Section 54(2):

If any person does any crime under sub-section 1 of this Act, he will be given penalty of maximum ten years rigorous imprisonment or fine upto 10 lacs Taka or for the both of the above.

Explanation: The meanings of the term used in section 54 are given below as explanation:

(i) "Computer Contaminant' means any set of computer instructions that are designed-

(a) To modify, destroy, record, transmit data, or programme residing within a computer, computer system or computer network; or

(b) By any means usurp the normal operation of the computer, computer system or computer network;

(ii) "Computer database" means a representation of the information, knowledge, facts, concepts or instructions in text, image, audio, video,-

(a) that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network;

(b) are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information data or programme that-

(a) destroys, damage, degrades or adversely affects the performance of a computer resource;

(b) attaches itself, to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify, or re-arrange any computer resource by any means.

8.3 Hacking with Computer System:

Hacking is a cyber crime. Unauthorised access of a computer system is generally termed as hacking. A amateur computer programmer usually commit this type of crime. Section 56 describes this crime and penalty for this crime:

According to section 56(1) following activities is termed as Hacking offence:

(a) With intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys, deletes, or alters, any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(b) Harm any computer, server, computer network, or any other electronic system by accessing it unlawfully and in which that person has no legal authority.

Penalty: According to section 56(2) whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka one crore or with both.

8.4 Online Pornography in Bangladesh:

Pornography is an offence in conventional law. The Penal Code 1860, section 293 define pornography is a punishable offence. Section 57 of the ICT Act 2006 clearly considers online pornography is also a punishable offence and determines the punishment for this crime. Nowadays pornography is a common in Bangladesh. But for the society of Bangladesh it is unwanted and unexpected. There are several pornographic website specially made for Bangladesh. Bangladeshi people made this websites. Some body thinks it the development in IT sector. But it destroys the ethics of Bangladesh and seriously injured the peaceful society of the country.

Most of the pornographic photos/moyies are taking by hidden camera, where the girls are not aware of it. Multi media, mobile phone are the main container of such photos and movies. Now there in no need to buy pornographic movies from VCD shops. There are a series of Bangladeshi website where pornographic films or movies are available. Now it become a very good business in Bangladesh.

In Bangladesh women and girls are the main victims of cyber pornography. But our Government is not taking adequate steps against cyber pornography. This will seriously affect our peaceful society of our country. So the provision under section 57 of the ICT Act 2006 should be implemented properly for the eradication of pornographic cyber crime from Bangladesh. So we thing implementation of the ICT Act is a must.

Child pornography is a part of cyber pornography. It is a serious cyber offence. It is individually recognised by the people of Bangladesh. Internet is a house hold commodity in Bangladesh. Its explosion has made the children a viable victim to the cyber crime. So intensity of this crime is becoming very dangerous for our society. As more homes have access to internet, their children might use internet and there has a chances of falling victim to the aggressive pedophiles. Generally the pedophiles use false identity to trap children. They may contact with them from chat room where they become friend. Then they obtain personal information from the innocent victims. The pedophiles also contract with the children on their E-mail address. These pedophiles use them for the purpose of sexual assault or use them as sex object. So it is a very series situation in Bangladesh. Our government and civil society should realise it and should take necessary protection and measure in this respect.

Section 57 of the ICT Act 2006 describes the provisions of cyber law and penalty for this offence as follows:

1. Offence: Whoever publishes or transmits or causes to be published or transmitted in electronic form any material which is obscene or if its effect is such as to tend to deprave and corrupt persons and which may harm the religious sentiment of the religious community and who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, then the work of that person shall be considered as a crime.

2. Penalty: If any person does such crime under sub-section 1 of the section he shall be punished on first conviction with imprisonment of either description for a term which may extend to 10 years and with fine which may extend to Taka one crore.

Chapter VIII

Part 2

Establishment of Cyber Tribunal, Enquiry, Trial and Appeal of crimes

9.1 Establishment of Cyber Tribunal:
9.2 Procedure of Trial in Cyber Tribunal,
9.3 Application of Criminal Procedure,
9.4 Rules regarding bail,
9.5 The time limit to give judgement,
9.6 The time limit of disputing a case by the tribunal,
9.7 Justice by session court,
9.8 The power of investigation of crime & Confession,
9.9 Power to arrest in a public places

9.1 Establishment of Cyber Tribunal:

The ICT Act 2006 of Bangladesh provided provisions to establish Cyber Tribunal for quick and effective trial of the cyber criminal committed crime under this Act. Section 58 of ICT Act 2006 provided provisions to establish Cyber Tribunal which are discussed as follows:

Section 58(1) stated that "Government by gazette notification, for the purpose of quick and effective trial of the crimes committed under the act, may establish one or more cyber tribunal, sometimes which is stated later as tribunal."

Section 58(2) stated that the cyber tribunal that is stated in sub-section (1) of the section will comprise of a session judge or an assistant session judge appointed by the Government with consultation with the supreme court; and such a judge appointed will be introduced "Judge, Cyber Tribunal".

Section 58(3) stated that 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.

Section 58(4) stated that 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.

9.2 Procedure of Trial by Cyber Tribunal:

Procedure of trial by Cyber Tribunal is described in section 69 of the ICT Act 2006. According to this Act the procedure are as follows:

Section 69(1) The special tribunal will not take any case for trial unless there is a written report by any police officer not under the rank of sub-inspector and approval of the controller or such person having authority from the controller for the purpose.

Section 69 (2) The tribunal during trial under the Act will follow Chapter 23 of the Coder of Criminal Procedure for trial in session court; provided that it will not be contradictory with this Act,

Section 69(3) Any tribunal for the purpose of justice if considered unnecessary without registering it can not stop the proceedings of a case.

Section 69(4) Where there is reason to believe for the tribunal that, the accused person is missing or hiding himself for which it is not possible to arrest him or there is less possibility to arrest him earlier, in that case the tribunal, by its order, may ask that person to present in the court by publishing it in two prominent Bengali Newspaper at a prescribed time and if that person fails to do so, the trial will be held with his absence.

Section 69(5) The accused person or the person having bail, after being present before the tribunal, if he is missing, or if he fails to present in front of the tribunal, the process stated in sub-section (4), will not be applicable and that tribunal with absence of the person try him registering its decision.

Section 69(6) If the person having bail or after presenting the court, fails to present before the court the procedure stated in sub-section 4 of the section shall not be applied and the tribunal may in written form give judgement without the presence of the accused.

Section 69(7) The tribunal on the bass of the application presented before it, or by its own effort , give the order to reinvestigate any case made under the Act and give the order to submit report in a prescribed time by the authority to any police official or in cases any person having the authority from the controller.

9.3 Application of Criminal Procedure:

According to section 70 of ICD Act 2006 The application of Criminal Procedure described as follows:

Section 70(1) The law of the Criminal Procedure, as per as possible, being not contrary to this Act will be applicable to the procedure of the tribunal and the tribunal will have all the original jurisdiction of the session judge.

Section 70(2) The advocate on be half of the government shall be known as the public prosecutor.

9.4 Rules regarding bail:

According to section 70 of ICD Act 2006 Rules regarding bail described as follows:

Section 71 stated that the judge of the cyber tribunal will not give bail to any person accused under the Act, unless-

(a) The government side is given scope for hearing on the grounds of the bail.

(b) The judge is satisfied that-

(1) There is enough ground to believe that the accused might not be proved guilty

(2) The crime is prima facie view is not too heavy and the punishment, even the crime is proved, will not be heard.

(c) He registers all those satisfactory grounds in written form.

9.5 The time limit to give judgement:

According to section 72 of ICD Act 2006 the time limit to give judgement described as follows:

Section 72(1) stated that the judge of the tribunal from the date of finishing examination of witness or evidence or hearing, whichever occurs later, will give judgement within ten days if he does not extend the time not more then 10 days with written reason for that.

Section 72(2) stated that when the judgement is given under sub-section of the section or if any appeal to the cyber appeal tribunal is made against the judgement then the copy of the appeal judgement will be sent to the controller by the cyber tribunal or appeal tribunal to reserve it according to the section 18(7) of the Act; if such any copy is sent the controller will take proper action to reserve it with proper process.

9.6 The time limit of disputing a case by the tribunal:

According to section 73 of ICD Act 2006, the time limit of disputing a case by the tribunal: described as follows:

Section 73(1) stated that the judge of the tribunal will complete the judgement procedure within 6months of filing the case.

Section 73(2) stated that if the judge fail to finish the case within the time prescribed under sub-section (1) of the section, he can increase the time limit not more then 3 months by stating written reasons behind the delay.

9.7 Justice by session court:

According to section 74 of ICD Act 2006, Justice by session court described as follows:

Section 74 stated that whatever may be in the Code of Criminal Procedure, unless special tribunal is formed, the crimes made under the Act shall be judged under Session Judge.

The procedure to be followed by the Session Judge described under section 75(1). This section stated that the session court will follow the section 23 of the Code of Criminal Procedure while judges judging the crimes under this Act.

Section 75(2) stated that whatever there may be in the Code of Criminal procedure, without the report of any official having the status not less than a sub-inspector and any prior approval of any official appointed by the controller for the purpose any session court as its original jurisdiction, will not take any case to judge.

9.8 The power of investigation of crime & Confiscation:

According to section 76 and 77 of ICD Act 2006, the power of investigation of crime & Confiscation described as follows

Section 76(1) stated that whatever may be in the code of criminal procedure, collector or any other official having authority from the collector or any police official having the rank not less lean sub-inspector will investigate the crimes under the Act.

Section 76(2) stated that the crimes under this Act shall be considered as non-cognizable.

Section 77 described Confiscation:

Section 77(1) stated that any computer, computer system, floppies, computer disks, tapes drives or any other accessories related therein respect

of which any provision of this Act, rules, regulations made there under has been or in being contravened to, in respect of which any offence has been committed, shall be liable to confiscation (Seizure by the government) by an order of the court tying an offence or contravention.

9.9 Power to arrest in a public places and procedure of Searching:

According to section 80 and 81 of ICD Act 2006, power to arrest in a public places and procedure of Searching described as follows

Section 80 stated that in the work of investigation under this Act, controller, any authorised person or any police officer not below the rank of an Inspector of police may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act by stating the reasons of searching in a written form.

Section 81 stated that if there is nothing contradictory in the Act, every investigation, notice, search, arrest or confiscation under this Act will follow the Code of Criminal Procedure.

Chapter VIII
Part 3

Establishment of Cyber Appeal Tribunal

10.1 Establishment of Cyber Appellate Tribunal:

10.2 Power and Procedure of Cyber Appellate Tribunal (CAT):

10.3 Characteristics of CAT

10.1 Establishment of Cyber Appellate Tribunal:

Section 82 of the ICT Act 2006 discussed about the establishment of Cyber Appellate Tribunal.

Section 82(1) stated that the government shall by notification in the official gazette; establish one of more appellate tribunals to be known as the Cyber Appellate Tribunal.

According to Section 82(2) the Cyber Appeal tribunal will be comprised of a chairman and two members appointed by the government.

According to Section 82(3) the chairman will be such person who was a justice of the Supreme Court or is continuing his post or capable to be 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.

According to Section 82(4) 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 Government.

10.2 Power and Procedure of Cyber Appellate Tribunal (CAT):

Section 83 of the ICT Act discuss about the power and procedure of Cyber Appellate Tribunal.

Section 83(1) stated that the Cyber Appellate Tribunal (CAT) shall have the power to here and settle the appeal made against the judgement of Cyber Tribunal and session court. So this Appellate has only Appeal jurisdiction only.

Section 83(2) Stated that in case of hearing and setting any appeal, the Cyber Appeal Tribunal will follow the rules made there under and if the procedure is not fixed by making rules, those rules with proper adoption will be followed which the high court division follow in case of criminal justice by the appeal tribunal.

Section 83(3) stated that the appeal tribunal will have the authority of supporting, canceling changing or editing the judgement of the cyber tribunal.

Section 83(4) stated that the decision of the appeal tribunal will be final.

10.3 Characteristics of CAT

1. These tribunals are lower in hierarchy to the High Court Division and higher in hierarchy to the adjudicating officer. The function of the adjudicating officer would be to hold an inquiry into whether any person has contravened the provisions of this Act and impose penalty to the offender, as per provision of this Act.

2. The court has no original jurisdiction.

3. It has vested with the powers of a civil court with the following functions:

a) Summon and examination of witnesses,

b) Require Production of documents,

c) Receive evidence,

d) Issue commission, and

e) Review its decision.

4. The CAT have appellate authority and facts finding authority,

5. The function of the CAT is to determine whether the provisions of the ICT Act 2006 have been contravened. For this one member of the CAT should have computer science background.

6. The CAT is involve with the following legal issue:

a) Application of Private International law to the different international parties relating to cyber dispute.

b) Jurisdictional Issues,

c) Interpretation of (i) cyber contractual dispute, (ii) Intellectual property dispute (iii) penal laws application, (iv) IT and ICT with related issues etc.

Chapter IX
Miscellaneous

11.1 Rule Making Power

Section 88, provides Rules making power to government. Under this provision the Government may, by Gazette notification or willingly on the Electronic Gazette, make rules to carry out the provisions of this Act.

(a) Method of attesting any document or data or doing so with electronic method.
(b) Submission, sanction of money by electronic method.
(c) Method of submitting or publishing electronic record.
(d) Pattern of digital signature and attaching this to other documents.
(e) Ability and experience of appointing controller, sub-controller and assistant controller and conditions of their service.
(f) Other standards followed by the controller.
(g) Matters that must be followed by the applicant.
(h) Tenure of the license.
(i) Pattern of application.
(j) Fees that is payable within the application form.
(k) Other attachments with the application form.
(l) Renewing form and the fees for that purpose.
(m) Pattern of application for digital signature certificate and necessary fees for that.
(n) Ability and experience of the members of appellate tribunal.

(o) Procedure of appeal.
(p) Procedure of investigation
(q) Other such necessary matters.

11.2 Regulation making Power

Section 89, provides Regulation making Power to government. Under this provision the Controller may, with the previous approval of the Government, by notification in the Official Gazette, or willingly on the electronic gazette notification make regulations consistent with this Act and the rules made there under to carry out the purposes of the Act

(a) The particulars relating to maintenance of database containing the disclosure record of every Certifying Authority.

(b) The conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority.

(c) Terms and conditions subject to which a licence may be granted.

(d) Other standards to be observed by a Certifying Authority.

(e) The manner in which the Certifying Authority shall disclose the matters.

(f) The particulars of statement which shall accompany an application.

11.3 The following Acts Need Modification

Cyber law is a new concept of law in the filed of Information Technology (IT) and Information and Communication Technology (ICT). IT and ICT has very wide aspect and influence over the modern technological developed society. The new and legal issues arise out related to Cyberspace, Computer Networks and Computer related problems. This legal issue has a multi-disciplinary dimension and includes the followings.

1. Law of Contract,
2. Law of Tort,
3. Intellectual Property,
4. Employment,
5. Telecommunications,

6. Sale of Goods,
7. Taxation,
8. Constitutional aspects,
9. Banking,
10. Evidence,
11. Police, Panel Laws,
12. Criminal Procedure,
13. Civil procedure,
14. Electronic Media, etc.

Computer network and inter net is a wide high way in the Cyberspace. The emergence of computer network and internet has raised numerous challenges and also involved with numerous legal issues. The new technological development involved the human society with various problems which arises various legal questions. Under these circumstances the modern countries required laws. For the end of justice and to control the external behavior of human relating to ICT, new legislative laws have come into force in different countries including Bangladesh.

To make a contract valid it is necessary to put a physical signature on the contract. For any business transaction it is also needed. For this the following Acts need modification to recognize digital signature valid.

32.2 The Evidence Act 1872:
32.3 The penal Code 1860
32.4 The Police Act 1861
32.5 The Bangladesh Bank Order 1972
32.6 The Bankers Books Evidence Act 1891
32.7 The Sales of Goods Act 1930,
32.8 The Contract Act 1872'
32.9 Cyber law and Tort Liability & Remedies,
32.10 The Copy Right Act 2000
32.11 The Telegraph Act 1885,
32.12 Cyberlaw and Consumer Protection Laws
32.13 Cyberlaw and Internet Taxation,

Statutory Cyber Laws

- **Information and Communication Technology Act, 2006**
- **ICT Policy in Bangladesh**
- **The (Indian) Information Technology Act 2000**
- **UNCITRAL Model Law on Economic Commerce United Nations Commission on International Trade Law (UNCITRAL)**
- **Bangladesh Telecommunications Regulations & Policies**
- **The Bangladesh Telecommunication Act, 2001**

An Un-official Manin Text of

INFORMATION AND COMMUNICATION TECHNOLOGY ACT, 2006

(ACT IXL of 2006)

8 October 2006

Whereas it is expedient to define and amend certain parts of law relating to legal recognition and security of Information and Communication Technology and related matters; it is hereby as enacted follows:

CHAPTER I

PRELIMINARY

"1. Short title, extent and commencement: (1) This Act may be called the "Information and Communication Technology Act, 2006."

(2) It shall extend to the whole of Bangladesh.

(3) It shall come into force immediately.

2. Definitions:- In this Act, unless the context otherwise requires,-

1. "Digital signature" means any data in electronic form that

a) Is attached with some other electronic data reasonably; and

b) Any justification of any digital signature will be done subject to the following conditions-

i) That is attached with the signer similarly.

ii) That is able to recognize the signer.

iii) That is created through such a secure method that can confirm the signer's control.

iv) That is attached to the data in such a way that it can recognize any change in the very data.

2) "Digital Signature Certificate" means a certificate issued under section 36 of this Act;

3) "Electronic" means electrical, digital, magnetic, wireless, optical, electromagnetic or any other such technology;

4) "Electronic data interchange" means transfer of data in electronic form from one computer to another computer with due transfer process for the purpose of gathering data.

5) "Electronic form", 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;

6) "Electronic Gazette" means the Official Gazette published in the electronic form;

7) "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;

8) "Internet" means such an international computer network through which users of computer, cellular phone or any other form of electronic method can exchange information and contact with each other and observe the content presented in the website;

9) "Electronic mail" means that mail that is formed in electronic method and sent and received through internet and such other papers;

10) "data" 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 been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

11) "Data message" means transfer electric of data including electronic and optical, any information formed, sent, received or reserved in the form of electronic mail, telegram, telex, tale-copy, short message (SMS) or in such other form;

12) "Website" means documents and information which can be browsed and observed by the user and that is reserved in the web server.

13) "Computer" 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;

14) "Computer network" means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line

or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

15) "Subscriber" means a person in whose name the Digital Signature Certificate is issued;

16) "Chairman" means the chairman of cyber appeal tribunal appointer under section 68 of the Act;

17) Civil Procedure" means the code of civil procedure, 1908 (Act V of 1908)

18) "Penal Code" means the penal code, 1860 (Act XLV of 1860;

19) "Determined" means that is determined by the rule;

20) "asymmetric cryptosystem" means a system capable for creating a signature under the conditions of section 17 of the Act.

21) "Controller" or "sub-controller" or "assistant Controller" means the "Controller" or "sub-controller" or "assistant Controller" of Certifying Authorities appointed under sub-section (1) of section 18 of this Act;

22) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(23) "Proving method: means that procedure which is used to identify the signature or proving the purity of any data message;

24) "Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

25) "Regulation" means the regulations made under the Act;

26) "Criminal procedure" means the Code of Criminal Procedure, 1898 (Act V of 1898);

27) "Person" means any person having natural personality, partnership business, samity, company, registered association and co-operative societies;

28) "Judge" means the judge of cyber tribunal under section 68 of the Act;

29) "Rules" means the rules given under this Act;

30) "Intermediary", with respect to any particular electronic message, means any person who on behalf of another person receives, tores or transmits that message or provides any service with respect to that message;

31) "Licence" means a licence granted to a Certifying Authority under section 22 of this Act;

32) "Attesting service provider" means the issuing authority of the certificate or any other authority giving any service related to digital signature;

33) "Certifying Authority" means a person who has been granted a license under section 22 of this Act to issue a Digital Signature Certificate;

4) "Certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

35) "Member" means the member of cyber appeal tribunal under section 82 of this Act;

36) "Signer" means any person gave signature through signature making machine or method;

37) "Signature proving machine" means the software or hard ware to justify the signature;

38) "Signature making machine" means the software or hardware to prepare the data for creating signature;

39) "Cyber Tribunal" or "Tribunal" means the tribunal made under the section 68 of the Act;

40) "Cyber Appeal Tribunal" means the Cyber Appeal Tribunal made under section 82 of this Act;

3. Superiority of the Act:- Whatever may be in any other Act having force at this time the provisions of this Act will take effect.

4. Extra regional effect of the Act:

1) If any person do any crime under the Act outside Bangladesh, if that had been done in Bangladesh, it would be punishable, in that case the Act will take effect in such way that the crime had been done in Bangladesh.

2) If any person with the help of any computer, computer system or computer network of Bangladesh do any crime in Bangladesh staying outside Bangladesh, in that case the provisions of the Act will take effecting such a way that the procedure of the crime had been done fully in Bangladesh.

3) If any person makes any crime to other place under this Act, staying in Bangladesh, in that case the provisions of the Act will take effect in such a way that the procedure of the crime had been done fully in Bangladesh.

Chapter II
DIGITAL SIGNATURE & ELECTRONIC RECORDS

5. Authentication of electronic records by digital signature:- (1) Subject to the provisions of section 2 of the Act, any subscriber may authenticate an electronic record by affixing his digital signature.

2) The authentication of the electronic record shall be effected by the use of asymmetric cryptosystem or recognized signature making machine or method.

6. Legal recognition of electronic records:- Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form then notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form: Provided that the information or any matter shall be accessible so as to be usable for a subsequent reference.

7. Legal recognition of digital signatures.- Where any law provides that-

1) Information or any matter shall be authenticated by affixing the signature; or

2) Any document shall be signed or bear the signature of any person;

hen, notwithstanding anything contain in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

8. Use of electronic records and digital signatures in Government and its agencies etc.- (1) Where any law requires-

30) "Intermediary", with respect to any particular electronic message, means any person who on behalf of another person receives, tores or transmits that message or provides any service with respect to that message;

31) "Licence" means a licence granted to a Certifying Authority under section 22 of this Act;

32) "Attesting service provider" means the issuing authority of the certificate or any other authority giving any service related to digital signature;

33) "Certifying Authority" means a person who has been granted a license under section 22 of this Act to issue a Digital Signature Certificate;

4) "Certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

35) "Member" means the member of cyber appeal tribunal under section 82 of this Act;

36) "Signer" means any person gave signature through signature making machine or method;

37) "Signature proving machine" means the software or hard ware to justify the signature;

38) "Signature making machine" means the software or hardware to prepare the data for creating signature;

39) "Cyber Tribunal" or "Tribunal" means the tribunal made under the section 68 of the Act;

40) "Cyber Appeal Tribunal" means the Cyber Appeal Tribunal made under section 82 of this Act:

3. Superiority of the Act:- Whatever may be in any other Act having force at this time the provisions of this Act will take effect.

4. Extra regional effect of the Act:

1) If any person do any crime under the Act outside Bangladesh, if that had been done in Bangladesh, it would be punishable, in that case the Act will take effect in such way that the crime had been done in Bangladesh.

2) If any person with the help of any computer, computer system or computer network of Bangladesh do any crime in Bangladesh staying outside Bangladesh, in that case the provisions of the Act will take effecting such a way that the procedure of the crime had been done fully in Bangladesh.

3) If any person makes any crime to other place under this Act, staying in Bangladesh, in that case the provisions of the Act will take effect in such a way that the procedure of the crime had been done fully in Bangladesh.

Chapter II

DIGITAL SIGNATURE & ELECTRONIC RECORDS

5. Authentication of electronic records by digital signature:- (1) Subject to the provisions of section 2 of the Act, any subscriber may authenticate an electronic record by affixing his digital signature.

2) The authentication of the electronic record shall be effected by the use of asymmetric cryptosystem or recognized signature making machine or method.

6. Legal recognition of electronic records:- Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form then notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form: Provided that the information or any matter shall be accessible so as to be usable for a subsequent reference.

7. Legal recognition of digital signatures.- Where any law provides that-

1) Information or any matter shall be authenticated by affixing the signature; or

2) Any document shall be signed or bear the signature of any person;

hen, notwithstanding anything contain in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

8. Use of electronic records and digital signatures in Government and its agencies etc.- (1) Where any law requires-

a) The filing of any form, application or any other document with any office, body, authority or agency owned or controlled by the Government in a particular manner;

b) The issue or grant of any licence, permit, sanction, approval or order by whatever name called in a particular manner;

c) The receipt or payment of money in a particular manner,

hen, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing issue, grant, receipt or payment, as the case may be, is affected by means of such electronic form as may be prescribed by the Government.

2) The Government may, for the purposes of sub- section (1) of this section, by rules, prescribe the manner and format in which such electronic records shall be filed, created or issued; the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record.

9. Retention of electronic records.- (1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:-

a) The information contained therein remains accessible so as to be usable for subsequent reference;

b) The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

rovided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

2) A person may satisfy the requirements referred to in sub - section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records.

10. Electronic Gazette.- Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette:

rovided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

11. No liability to accept documents in electronic form.- Nothing contained in this Act shall confer a right upon any person to insist that any Ministry or department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

12. Power to make rules by Government in respect of digital signatures.- The Government may, for the purpose of this Act, by rules, prescribe in the electronic Gazette or official Gazette:

a) The type of digital signature;

b) The manner and format in which the digital signature shall be affixed;

c) The manner or procedure which facilitates identification of the person affixing the digital signature;

d) The control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

e) Any other matter which is necessary to give legal effect to digital signatures.

CHAPTER III
ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

13. Attribution. - (1) An electronic record shall be that of the originator if it was sent by the originator himself.

2) As between the originator and the addressee, an electronic record shall be deemed to be that of the originator if it was sent-

a) By a person who had the authority to act on behalf of the originator in respect of that electronic record; or

b) By an information system programmed by or on behalf of the originator to operate automatically.

3) As between the originator and the addressee, an addressee shall be entitled to regard an electronic record as being that of the originator and to act on that assumption if-

a) In order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

b) The information as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify the electronic records as its own.

4) Sub-section (3) of this section shall not apply-

a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using reasonable care or using any agreed procedure, that the electronic record was not that of the originator; or

c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator or the addressee is entitled to act on the assumption, then, as between the originator and the addressee,

the addressee shall be entitled to regard the electronic record received as being what the originator intended to send and tp act on that assumption:

(6) Whatever is stated in section (5) the addressee shall not be so entitled when the addressee knew or should have known, after exercising reasonable care or using any agreed procedure that the transmission resulted in any error in the electronic record as received.

7) The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption. But this will not be applicable on the following records,

a) If the addressee duplicate another electronic record or

b) If addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate.

14. Acknowledgement of receipt.- (1) Sub- sections (2) (3) and (4) of this section shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –

a) Any communication by the addressee, automated or otherwise; or

b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

3) Where the originator has stipulated that the electronic record shall be conditional on receipt of the acknowledgement, then, until the acknowledgement has been received, the electronic record shall be deemed to have been never sent by the originator.

4) Where the originator has not stipulated that the electronic record shall be conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator-

a) May give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

b) If no acknowledgement is received within the time specified in clause (a) of this sub-section, may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

5) Where the originator receives the addressee's acknowledgement of receipt, it shall be presumed that the related electronic record was received by the addressee, but that presumption shall not imply that the content of the electronic record corresponds to the content of the record received.

6) Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it shall be presumed that those requirements have been met.

15. Time and place of dispatch and receipt of electronic record.-

(1) When the originator and the addressee not agreed otherwise-

(a) The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(b) The time of receipt of an electronic record shall be determined as follows, namely-

(I) If the addressee has designated a computer resource for the purpose of receiving electronic records, receipt occurs,-

(i) At the time when the electronic record enters the designated computer resource; or

(ii) If the electronic record is sent to a computer resource of the addressee that is not designated computer resource, at the time when the electronic record is retrieved by the addressee;

(II) If the addressee has not designated a computer resource along with specified timing, if any, receipt occurs when the electronic record enters the computer resource of the addressee,

(c) An electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(2) Though the provisions of sub-section 1(c) regarding electronic device or system or the place of source of computer is different from sub-section 1(b), the later one shall apply.

(3) For the purpose of this section,-

(a) If the originator or the addressee has more than one place of business, the principle place of business shall be the place of business;

(b) If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

Explanation: in case of any registered organization 'the principal place of business" or "usual place of residence" means the place where it is registered.

CHAPTER IV
SECURE ELECTRONIC RECORDS & SECURE DIGITAL SIGNATURES

16. Secure electronic record. - Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

17. Secure digital signature: (1) If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

(a) Unique to the person affixing it;

(b) Capable of identifying the person affixing it;

(c) Created in a manner or using a means under the sole control of the person affixing it'

Then such electronic signature shall be deemed to be a secure electronic signature subject to sub-section (2), of the Act.

(2) Though the provision of sub-section (1), the electronic signature would be invalidated, the electronic record was altered.

CHAPTER V
CONTROLLER & CERTIFYING AUTHORITIES

18. [1][Controller and other officers etc.—Whereas it is expedient tc fullfil the objectives of this Act, Government by Gazette notification and willingly to Electronic Gazette Notifications, may appoint a Controller, and required to of Deputy Controller and Assistant Controller as per terms and conditions of the Gazette Notifications:

---

[1]। তথ্য ও যোগাযোগ প্রযুক্তি (সংশোধন) আইন, ২০০৯ (২০০৯ সনের ৪১নং আইন) এর ২ ধারাবলে উপ-ধারা (১ এবং উপাত্তটীকা প্রতিস্থাপিত।

Provided that, the period will not be more then one year from the dates of Notification.]

(2) The Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.

(3) The Deputy Controllers and the Assistant Controllers shall perform such functions as are assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Government.

(5) The Head Office of the Controller shall be in Dhaka and Branch Offices of the office of the Controller shall be at such places as the Government may specify and may be established at such places as the Government may think fit for any specific time decided by the Government.

(6) There shall be a seal of the office of the Controller as the Government may specify.

(7) Under this Act, there shall be a room for reserving all electronic record in the controller's office and these rooms shall be called "electronic reservation room".

19. Functions of the Controller. - The Controller may perform all or any of the following functions, namely:-

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys o f the Certifying Authorities;

(c) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(d) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(e) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certifying and the public key;

(f) Specifying the form and content of a Electronic Signature Certificate and the key;

(g) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(h) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them

(i) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(j) Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(k) Resolving any conflict of interests between the Certifying Authorities and the subscribers;

(l) Laying down the duties and responsibilities of the Certifying Authorities;

(m) Resolving the computerized data that can:

(i) Maintaining database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations,

(ii) Be accessible to the members of the public.

(n) Performing those works laid by this works or any work laid by any other Act.

20. Recognition of foreign Certifying Authorities.- (1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1) of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub -section (1) of this section, he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

21. Controller to act as repository.- (1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall ensure that the secrecy and security of the digital signatures are assured and in order to do so he shall make use of hardware, software and procedures that are secure from misuse and observe such other standards as may be prescribed by the Government.

22. Licence to issue Digital Signature Certificates.- (1) Subject to the provisions of sub-section (2) of this section, any person may make an application to the Controller for a licence to issue Electronic Signature Certificates.

(2) No licence shall be issued under sub- section (1) of this section unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary to issue Digital Signature Certificates as may be prescribed by the Government.

(3) A license granted under sub -section (1) of this section –

(a) Shall be valid for such period as may be prescribed by the Government;

(b) Shall be subject to such terms and conditions as may be specified;

(c) Shall not be transferable or heritable.

23. Application for license.- (1) Every application for issue of a license shall be in such form as may be prescribed by the Government.

(2) Every application under sub-section (1) of this section, for issue of a license shall be accompanied by –

(a) A certification practice statement;

(b) A statement including the procedures with respect to identification of the applicant;

(c) Proof papers of payment of various fees;

(d) Such other documents as may be prescribed by the Government.

24. Renewal of licence.- Any license issued under this Act shall be renewed automatically for a prescribed period subject to paying the fixed price.

25. Procedure for grant or rejection of licence.- The Controller may, on receipt of an application under sub-section (1) of section 22 of this Act, after considering the documents accompanying the application and such other factors as he deems fit, grant the license or reject the application.

26. Revocation and suspension of licence.- (1) Subject to other provisions of the Act, the Controller may nullify or stop any license, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has –

(a) Made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;

(b) Failed to comply with the terms and conditions subject to which the license was granted;

(c) Failed to maintain the standards specified under clause (b) of subsection (2) of section 21 of this Act;

(d) Contravened any provisions of this Act, rules, regulations or orders made thereunder;

(2) Under sub-section (1) of this section no license can be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(3) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1) of this section by order, suspend such license pending the completion of any enquiry ordered by him.

(4) Under sub-section (3) of this section no license shall be suspended for a period exceeding fourteen days unless the certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(5) A Certifying Authority whose licence has been suspended shall not issue any Electronic Signature Certificate during the period of such suspension.

27. Notice of suspension or revocation of licence.- (1) Where the license of a Certifying Authority is revoked or suspended, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such revocation or suspension, as the case may be, in all such repositories:

Provided that the database containing the notice of such revocation or suspension, as the case may be, shall be made available through a website which shall be accessible round the clock for all the citizens.

28. Power to delegate.- The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any other officer to exercise any of the powers of the Controller under this Chapter.

29. Power to investigate.- (1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall, for the purposes of sub- section (1) of this section, have the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908, (Act V of 1908), when trying a suit in respect of the following matters, namely:-

(a) Discovery and inspection;

(b) Enforcing the attendance of any person and examining him on oath or affirmation;

(c) Compelling the production of any documents; and

(d) Issuing commissions for the examination of witness.

30. Access to computers and data.- (1) Without prejudice to the provisions of section 45 of this Act, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purpose of sub -section (1) of this section, the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

31. Certifying Authority to follow certain procedures.- Every Certifying Authority shall, -

(a) Make use of hardware, software, and procedures that are secure from intrusion and misuse;

(b) Provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) Observe such other standards as may be specified by regulations.

32. Certifying Authority to ensure compliance of the Act, rules, regulations, etc. - Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations or orders made thereunder.

33. Display of license.- Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carriers on its business.

34. Surrender of license.- Every Certifying Authority whose license is revoked or suspended shall immediately after such revocation or suspension, surrender the license to the Controller.

35. Disclosure of certain matters.- (1) Every Certifying Authority shall disclose in the manner specified by regulations such as:–

(a) For certifying another Electronic Signature Certificate that Electronic Signature Certificate that is used by Certifying Authority.

(b) Any certification practice statement relevant thereto;

(c) Notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) Any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Certifying Authority has issued, or the Certifying Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall use reasonable efforts to notify any person who is likely to be affected by the occurrence; or act in accordance

with the procedure specified in its certification practice statement to deal with such event or situation.

36. Issue of certificate.- (1) The Certifying Authority may issue a certificate to a prospective subscriber only after the Certifying Authority.

(a) Has received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber; and

(b) Has a certificate practice statement, complied with all the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber;

(c) Has confirmed by itself or through as authorised agent that the prospective subscriber is the person to be listed in the certificate to be issued;

(d) Has the confirmation of the information in the certificate to be issued is accurate: the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) Has been paid such fees prescribed for issuance of certificate.

37. Assurance by certifying authority: (1) By issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement under sub-section (1) of this section, the certifying Authority represents that it has confirmed that –

(a) the Certifying Authority has complied with all applicable requirements of this Act and the rules and regulations made thereunder in issuing the certificate, and if the Certifying Authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(b) All information in the certificate is accurate, unless the Certifying Authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(c) The Certifying Authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in clauses (a) to (b) of this subsection.

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, sub -section (2) of this section shall apply to the extent that the representations are not inconsistent with the certification practice statement.

38. Revocation of Digital Signature Certificate.- (1) A Certifying Authority shall revoke a Digital Signature Certificate issued by it on the following grounds.

(a) Where the subscriber or any person authorised by him makes a request to that effect; or

(b) Upon the death o f the subscriber;

(c) Where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub -section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that -

(a) A material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) A requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) The Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) The subscriber has been declared insolvent by a competent Court or authority.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Suspension of Digital Signature Certificate.- (1) Subject to the provisions of sub -section (2) of this section, the Certifying Authority

which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate under the following grounds.

(a) On receipt of a request to that effect from the subscriber listed in the Digital Signature Certificate; or Any person duly authorised to act on behalf of that subscriber;

(b) If it is of opinion that the Digital Signature Certificate should be suspended in public interest by the certifying authority.

(2) A Digital Signature Certificate shall not be suspended under sub-section 1(b) without giving a notice of 30 days to the concerned authority.

(3) As an effect of the measure taken by the authority, under sub-section 2 of the section, if the Certifying Authority is not satisfied with the response of the subscriber, the authority can suspect the license. .

(4) The Certifying Authority may inform the subscriber after suspending such Digital Signature Certificate.

40. Notice of revocation or suspension. - (1) Where a Digital Signature Certificate is revoked under section 38 of this Act or suspended under section 39 of this Act, the Certifying Authority shall publish a notice of such revocation or suspension, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such revocation or suspension, as the case may be, in all such repositories.

CHAPTER VI
DUTIES OF SUBSCRIBERS

41. Appling the security procedure. – Where any Digital Signature Certificate the public key of which corresponds to the private key of their subscriber which is to be listed in the Digital Signature Certificate has been accepted by the subscriber, the subscriber shall generate that key pair applying the security procedure.

42. Acceptance of Digital Signature Certificate.- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate to one or more persons; or in a repository; or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

(a) All representations made by the subscriber to the Certifying Authority and all materials relevant to the information contained in the Digital Signature Certificate are true; and

(b) All information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

43. Obtaining Digital Signature Certificate.- All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

44. Control of private key.- (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in such manner as may be specified by regulations.

CHAPTER VII
PENALTIES AND ADJUDICATION

45. Power of Controller to Order: To ensure the implementation of the Act or any rules under the Act or any rules under the Act, the controller, by his order, may compel or restrict any certifying authority or any of its employees regarding any work that seems to be fit by the controller.

46. Power of controller to order in emergency time: (1) If the Controller is satisfied on the grounds that are necessary to give any order for practicing the sovereignty, unity, security of Bangladesh, the relationship with the other countries and public welfare of the country

or for the purpose of controlling any crime under this Act, the controller may give order to any law enforcing authority for restricting of telecasting any data with the help of any computer system provided that the reasons behind the order should be written on the order form.

(2) If any order is made under the sub-section (1), any subscriber or his authority will be bound to help the prescribed authority by the controller to decrypt any data necessary.

t47. **Power to announce any reserved system.**- (1) The Controller may with the authority of the Government or willingly using the electronic gazette, declare any computer, computer system or computer network as the reserved system.

(2) For the purpose sub-section (1), for securing the declared reserved system, the controller with written order may give a person the authority to do the work.

48. Penalty for failure to furnish document, return or report.- Whoever fails to furnish any document, return or report to the Controller or the Certifying Authority which he is required under this Act, or rules or regulations made thereunder to furnish shall be liable to pay a penalty which may extend to Taka two lakh for each such failure.

49. Penalty for failure to file return, information, books, etc.- Whoever fails to file any return or furnish any information, books or other documents within the time specified therefore in this Act, or rules or regulations made thereunder the controller or any person authorised by the government may give an order to pay a penalty which may extended to take ten thousand for every day during which such failure continues.

50. Penalty for failure to maintain books of accounts or records.- Whoever fails to maintain books of account or records which he is required under this Act, or rules or regulations made thereunder, the controller or any person authorised by the government may give an order to pay a penalty which may extended to taka twolacs.

51. Residuary penalty.- Whoever contravenes any rules or regulation made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay compensation, made in a written form provided with reasonable grounds behind the penalty, the

penalty not exceeding Taka twenty five thousand by such contravention, by the controller or any person authorised by the government.

52. The prohibitory power of the controller to restrict possible infringement of the Act.- (1) If the controller thinks fit that a person had endeavored such a work that may infringe any rules and regulations made under this Act, he (the controller) may give such order to show reasonable cause why he will not be stopped from doing the work within prescribed time limit, and when such reason is submitted, the controller may give order to stop the work or any other order whatever he thinks fit relating the fact.

(2) It the Controller is satisfied on the ground that any infringement under section (1) or nature of infringement is such a type that it requires immediate action, then the controller at the time of serving notice under the controller's discretion can give an interim order of stay on that ground and that would be continued till any permanent decision is determined by the controller.

(3) If any order is given under sub-section (1) and (2) to be followed by any person, then the person is bound to follow the order.

(4) If any person infringes any order under this section, the controller can fine him up to ten thousand taka.

53. Fine.-(1) In addition to the fine mentioned under this Act , the controller may impose fine for infringement of rules or regulations made there under.

(2) Any fine under this Act cannot be made by the controller to any person without giving him the chance of hearing with reasonable hearing.

(3) Within seven days of giving fine to a person by the controller, the aggrieved person may apply to the controller for re-considering the fine given and the controller within 15 days will settle the matter by giving the aggrieved person a reasonable opportunity of hearing.

(4) If fine made under this Act is not paid then it will be considered Actionable as government deemed under Public Demand Recovery Act 1913 (Bengal Act III of 1913).

CHAPTER VIII

CRIME, INVESTIGATION, JUDGEMENT AND PUNISHMENT

Part 1

Crime and Punishment

54. Penalty for damage to computer, Computer system, etc.- (1) If any person, without permission of the owner or any other person who is in charge of a computer, computer system, computer network,-

(a) Accesses or secures access to such computer, computer system or computer network for the purpose of having data or destroy it;

(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) Introduce or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damage or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any such computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised 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, or rules and regulations made there under;

(h) Willingly without the permission of the receiver or the sender, to advertise any service or commodities, produce or make marketing of span or try to do it or send mails unnecessarily;

(i) Change the services availed of by a person to the account of another person by tempering with or manipulating any computer, computer system or computer network;

Then the act of that person shall be considered to be a crime under this Act.

(2) If any person does any crime under sub-section 1 of this Act, he will be given penalty of maximum ten years rigorous imprisonment or fine upto 10 lacs Taka or for the both of the above.

Explanation: For the purpose of this section,-

(i) "Computer Contaminant' means any set of computer instructions that are designed-

(a) To modify, destroy, record, transmit data, or programme residing within a computer, computer system or computer network; or

(b) By any means usurp the normal operation of the computer, computer system or computer network;

(ii) "Computer database" means a representation of the information, knowledge, facts, concepts or instructions in text, image, audio, video,-

(a) that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network;

(b) are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information data or programme that,-

(a) destroys, damage, degrades or adversely affects the performance of a computer resource;

(b) attaches itself, to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify, or re-arrange any computer resource by any means.

55. Punishment for tampering with computer source documents.- (1) Whoever intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by any law for the time being in force, shall be punishable.

(2) If any person does a crime under sub-section 1 of this section he will br given imprisonment of either description for a term which may extend to three years, or with fine which may extend to taka three lacs, or with both.

Explanation.- For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

56. Hacking with computer system. – (1) If whoever,

(a) With intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys, deletes, or alters, any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(b) Harm any computer, server, computer network, or any other electronic system by accessing it unlawfully and in which that person has no legal authority;

He commits the offence of "hacking".

(2) Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka one crore or with both.

57. Punishment for publishing obscene information in electronic form.- (1) Whoever publishes or transmits or causes to be published or transmitted in electronic form any material which is obscene or if its effect is such as to tend to deprave and corrupt persons and which may harm the religious sentiment of the religious community and who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, then the work of that person shall be considered as a crime.

(2) If any person does such crime under sub-section 1 of the section he shall be punished on first conviction with imprisonment of either description for a term which may extend to 10 years and with fine which may extend to Taka one crore.

58. Punishment for failure to surrender license.- (1) Where any Certifying Authority fails to surrender a license under section 34 of this Act, the person in whose favour the license is issued shall be guilty of an offence.

(2) If any person does any crime under sub-section 1 of the section, he shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to Taka ten thousand or with both.

59. Punishment for failure to comply with order made by the controller.- (1) The controller may, by order direct a Certifying Authority or any employee of such a Certifying Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, or rules and regulations made there under and if any person fails to comply with any order made hereunder of this Act shall be guilty of an offence.

(2) If any person makes any crime under sub-section (1) of the section, he shall be liable on conviction to suffer imprisonment of either description for a term which may extend to one year or to pay a fine which may extend to Taka one lakh or to both.

60. Penalty for violation of the order of the controller in emergency time: (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, pr security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. If any body does so it will be considered to be a crime.

(2) If any person makes any crime under sub-section (1) of the section, he shall be punished with imprisonment of either description for a term which may extend to five years or to pay a fine which may extend to Taka 5 lakh or with both.

61. Crime and punishment for unauthorized access to protect system.- (1) The Controller may, by notification in the Official Gazette or willingly in electronic gazette declare any computer, computer system or computer network to be a protected system. Even that if any person enters into those computer, computer system or computer networks illegally then it will be considered as a crime.

(2) If any person does any crime under sub-section (1) of the section he shall be punished with imprisonment of either description

for a term which may extend to ten years or with fine which may extend to Taka 10 lakh or with both.

62. Punishment for false representation and hiding information: (1) Whoever makes any false representation and do the work of hiding information to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate then the act will be a crime.

(2) If any person makes any crime under sub-section (1) of the section, as the case may be, he shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to Taka 2 lakh or with both.

63. Crime and punishment on discloser of confidentiality and privacy: (1) Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the power conferred under this Ac, or rules and regulations made there under, has secured across 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. If any person does so, his work will be considered as crime.

(2) If any person does crime under sub-section (1) of the section he shall be punished with imprisonment of either description for a term which may extend to two years or with fine, which may extend to Taka 2 lakh or with both.

64. Crime and punishment on publishing false Digital Signature Certificate.- No person shall publish a Digital Signature Certificate or otherwise make it available to any other person knowing that,

(a) The Certifying Authority listed in the certificate has not issued it; or

(b)The subscriber listed in the certificate has not accepted it, or

(c) The certificate has been revoked or suspended,

Unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation. If this is done violating the sub-section (1) of this section, it will be considered as a crime.

65. Crime and punishment for publication of Digital Signature Certificate for fraudulent purpose.- (1) Whoever knowingly creates, publishes or otherwise makes available a digital Signature Certificate for any fraudulent or unlawful purpose, this work shall be a crime.

(2) If any person does crime under sub-section (1) of the section he shall be punished with imprisonment of either description for a term which may extend to two years or with fine, which may extend to Taka 2 lakh or with both.

66. Crime and punishment for using computer for committing an offence.- (1) Whoever uses or intentionally causes to be used a computer, computer network, computer resource or computer system for, or for facilitating, the commission of a crime, this work shall be considered as a crime.

(2) If any person makes a crime under sub-section (1) of the section, he shall be punished according to the punishment prescribed for the main crime that was the sole purpose of the crime under sub-section (1) of the section.

67. Offences committed by companies.- (1) Where a person committing an offence under this Act, or rule and regulation made thereunder or a contravention of any provision of this Act, rule, regulation, direction or order made thereunder is a company, every person who, at the time the offence or the contravention, as the case may be, was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the offence or the contravention, as the case may be, and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub -section shall render any such person to punishment if he proves that the offence or contravention was committed without his knowledge or that he exercised due diligence in order to prevent commission of such offence or contravention.

Explanation.- For the purposes of this section.-

(a) "Company" means any body corporate and includes a firm or other association of individuals; and

(b) "Director", in relation to a firm, includes a partner and directors of the directory board in the firm."

Part 2

Establishment of Cyber Tribunal, Enquary, Trial and Appeal of Cremes etc.

68. Establishment of Cyber Tribunal.- (1) Government by gazette notification, for the purpose of quick and effective trial of the crimes committed under the act , may establish one or more cyber tribunal, sometimes which is stated later as tribunal.

(2) The cyber tribunal that is stated in sub-section (1) of the section will comprise of a session judge or an assistant session judge appointed by the Government with consultation with the Supreme Court; and such a judge appointed will be introduced "Judge, Cyber Tribunal".

(3) 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.

(4) 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.

69. Procedure of trial of the Cyber tribunal.- (1) The special tribunal will not take any case for trial unless there is a written report by any police officer not under the rank of sub-inspector and approval of the controller or such person having authority from the controller for the purpose.

(2) The tribunal during trial under the Act will follow Chapter 23 of the Coder of Criminal Procedure for trial in Session Court; provided that it will not be contradictory with this Act,

(3) Any tribunal for the purpose of justice if considered unnecessary without registering it can not stop the proceedings of a case.

(4) Where there is reason to believe for the tribunal that, the accused person is missing or hiding himself for which it is not possible to arrest him or there is less possibility to arrest him earlier, in that case the tribunal, by its order, may ask that person to present in the Court by publishing it in two prominent Bengali Newspaper at a prescribed time and if that person fails to do so, the trial will be held with his absence.

(5) The accused person or the person having bail, after being present before the tribunal, if he is missing, or if he fails to present in front of the tribunal, the process stated in sub-section (4), will not be applicable and that tribunal with absence of the person try him registering its decision.

(6) If the person having bail or after presenting the Court, fails to present before the Court the procedure stated in sub-section 4 of the section shall not be applied and the tribunal may in written form give judgement without the presence of the accused.

(7) The tribunal on the bass of the application presented before it, or by its own effort , give the order to reinvestigate any case made under the Act and give the order to submit report in a prescribed time by the authority to any police official or in cases any person having the authority from the controller.

70. The application of Criminal Procedure in the procedure of the Tribunal.- (1) The law of the Criminal Procedure , as per as possible, being not contrary to this Act will be applicable to the procedure of the tribunal and the tribunal will have all the original jurisdiction of the session judge.

(2) The advocate on be half of the government shall be known as the public prosecutor.

71. Rules regarding bails.- The judge of the cyber tribunal will not give bail to any person accused under the Act, unless-

(a) The government side is given scope for hearing on the grounds of the bail.

(b) The judge is satisfied that-

(1) There is enough ground to believe that the accused might not be proved guilty

(2) The crime is prima facie view is not too heavy and the punishment, even the crime is proved, will not be heard.

(c) He registers all those satisfactory grounds in written form.

72. The time limit to give judgement.- (1) The judge of the tribunal from the date of finishing examination of witness or evidence or hearing, whichever occurs later, will give judgement within ten days if he does not extend the time not more then 10 years with written reason for that.

(2) When the judgement is given under sub-section of the section or if any appeal to the cyber appeal tribunal is made against the judgement then the copy of the appeal judgement will be sent to the controller by the cyber tribunal or appeal tribunal to reserve it according to the section18(7) of the Act; if such any copy is sent the controller will take proper action to reserve it with proper process.

73. The time limit of disputing a case by the tribunal.- (1) The judge of the tribunal will complete the judgment procedure within 6months of filing the case.

(2) If the judge fail to finish the case within the time prescribed under sub-section (1) of the section, he can increase the time limit not more then 3 months by stating written reasons behind the delay.

3) if the Judge fails to finish a case within the time limit under sub-section (2) of this section, he may continue the process by submitting a paper to High Court and the controller sating the reasons behind the delay.

74. Justice by Session Court.-Whatever may be in the Code of Criminal Procedure, unless special tribunal is formed, the crimes made under the Act shall be judged under Session Judge.

75. The procedure to be followed by the Session Judge.- (1) The Session Court will follow the section 23 of the Code of Criminal Procedure while judges judging the crime s under this Act.

(2) Whatever there may be in the Code of Criminal procedure, without the report of any official having the status not less than a sub-inspector and any prior approval of any official appointed by the controller for the purpose any Session Court as its original jurisdiction, will not take any case to judge.

76. The power of investigation of crime etc.- (1) Whatever may be in the code of criminal procedure , collector or any other official having authority from the collector or any police official having the rank not less lean sub-inspector will investigate the crimes under the Act.

(2) The crimes under this Act shall be considered as non-cognizable.

77. Confession: (1) Any computer, computer system, floppies, computer disks, tapes drives or any other accessories related therein respect of which any provision of this Act, rules, regulations made there under has been or in being contravened to, in respect of wh 360 any offence has been committed, shall be liable to confiscation by an order of the Court tying an offence or contravention.

(2) If the Court has the satisfaction that the person is whose possession, power or control any such computer, computer system,

floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this ac, rules, orders or regulations made there under, the confiscation will not take effect.

(3) If any legal computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found with the confiscated computer, computer system, floppies, compact disks, tape drive or any other accessories relating thereto the legal ones will also be confiscated.

(4) Whatever may be in this system, if at the time of doing crime under sub-section (1) of the section, any computer or any related things of any government or registered government official is used, then those will not be confiscated.

78. Penalties or confiscation no bar against other punishment.- No penalty impose or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby may be liable under any other law for the time being in force.

79. Network service providers not to be liable in certain cases.- For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, or rules or regulations made there under, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation: For the purpose of this section.-

(a) "Network service provider" means an intermediary,

(b) "Third party information" means any information dealt with by a network service provider with his capacity as an intermediary.

80. Power to arrest in a public places.- In the work of investigation under this Act, controller, any authorised person or any police officer not below the rank of an Inspector of police may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act by stating the reasons of searching in a written form.

81. The procedure of Searching etc.- If there is nothing contradictory in the Act, every investigation , notice, search, arrest or confiscation under this Act will follow the code of criminal procedure.

Part 3
ESTABLISHMENT OF CYBER APPEAL TRIBUNAL ETC

82. Establishment of Cyber Appellate Tribunal.- (1) The government shall by notification in the official gazette, establish one of more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Cyber Appeal tribunal will be comprised of a chairman and two members appointed by the government.

(3) The chairman will be such person who was a justice of the Supreme Court or is continuing his post or capable to be 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.

(4) 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 Government.

83. Procedure and power of Cyber Appellate Tribunal.- (1) The Cyber Appellate Tribunal shall have the power to here and settle the appeal made against the judgement of Cyber Tribunal and Session Court.

(2) In case of hearing and setting any appeal, the Cyber Appeal Tribunal will follow the rules made there under and if the procedure is not fixed by making rules, those rules with proper adoption will be followed which the high Court Division follow in case of criminal justice by the appeal tribunal.

(3) The appeal tribunal will have the authority of supporting, canceling changing or editing the judgement of the cyber tribunal.

(4) The decision of the appeal tribunal will be final.

84. Appealing procedure in case of not establishing cyber appeal tribunal.- Under this part of the Act if the Cyber Appeal Tribunal is not established, what ever may be in the code of criminal procedure appeal may be made t high Court Division of the Supreme Court against judgement of Session Judge s or Cyber Tribunal.

CHAPTER IX
MISCILINIOUS

85. Public Servant.- The controller, sub-controller, assistant controller or any other such person under the Act will be recognised as public servant within the meaning of of section 21 of the penal code.

86. Protection of action taken in good faith.- No suit, prosecution or other legal proceedings shall lie against the Government, the Controller or any person acting on his behalf, the Presiding Officer of the Cyber Appellate Tribunal, the Adjudicating Officers, and the staff of the Presiding Officer of the Cyber Appellate Tribunal, the Controller and the Adjudicating Officers for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation, order or direction made there under.

87. The use of extensive meaning in case of certain Acts.- To fulfill the purpose of the Act,

(a) The word "document" in section 29 of the Penal Code 1890will includes the document created by the electronic method or method.

(b) The word "document" in section 3 of the Evidence Act. 1872 will include the document created by electronic method or machine.

(c) The term "Bankers Book" in clause (3) , section 2 of the Bankers Books Evidence Act, 1892 will include ledgers, day-books, cash books, account books, and all other books by electronic machine.

88. Rules making power.- The Government may, by Gazette notification or willingly on the Electronic Gazette, make rules to carry out the provisions of this Act.

(a) Method of attesting any document or data or doing so with electronic method.

(b) Submission, sanction of money by electronic method.

(c) Method of submitting or publishing electronic record.

(d) Pattern of digital signature and attaching this to other documents.

(e) Ability and experience of appointing controller, sub-controller and assistant controller and conditions of their service.

(f) Other standards followed by the controller.

(g) Matters that must be followed by the applicant.

(h) Tenure of the license.

(i) Pattern of application.

(j) Fees that is payable within the application form.

(k) Other attachments with the application form.

(l) Renewing form and the fees for that purpose.

(m) Pattern of application for digital signature certificate and necessary fees for that.

(n) Ability and experience of the members of appellate tribunal.

(o) Procedure of appeal.

(p) Procedure of investigation

(q) Other such necessary matters.

89. Regulation making Power.- The Controller may, with the previous approval of the Government, by notification in the Official Gazette, or willingly on the electronic gazette notification make regulations consistent with this Act and the rules made there under to carry out the purposes of the Act

(a) The particulars relating to maintenance of database containing the disclosure record of every Certifying Authority.

(b) The conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority.

(c) Terms and conditions subject to which a licence may be granted.

(d) Other standards to be observed by a Certifying Authority.

(e) The manner in which the Certifying Authority shall disclose the matters.

(f) The particulars of statement which shall accompany an application.

90. Original and English Text.- The original text of the Act shall be in Bengali and there shall be reliable English text, provided that in the event of conflict between Bengali and English, Bengali text shall prevail.

ICT POLICY IN BANGLADESH

National Information and Communication Technology (ICT) Policy
(October: 2002)

Ministry of Science and Information & Communication Technology
Government of the People's Republic of Bangladesh

1.0 Preamble

1.1 Information Communication Technology (ICT) encompasses the broad fields of data/information processing, transmission and communications by means of computer and telecommunication techniques and these modern tools are being increasingly used for organizational/personal information processing in all sectors of economy and society. This document presents the policy guidelines for the development of the ICT sector in Bangladesh.

1.2 A dependable information system is essential for efficient management and operation of the public and private sectors.

But there is a shortage of locally generated information needed for efficient performance of these sectors. In order to meet this objective, ICT use in every sector shall have to be accelerated in terms of information generation, utilization and applications. Considering the gravity and importance of ICT Hon'ble Prime Minister has already declared ICT as the thrust sector.

1.3 Over the last few years, many nations have taken advantage of the opportunities afforded by ICT within a policy framework, laid down guidelines and preceded with the formulation of a national ICT strategy as a part of the overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development.

2. 0 Vision and Objectives

2.1 Vision: This Policy aims at building an ICT-driven nation comprising of knowledge-based society by the year 2006. In view of this, a country-wide ICT-infrastructure will be developed to ensure access to information by every citizen to facilitate empowerment of people and enhance democratic values and norms for sustainable economic development by using the infrastructure for human resources development, governance, e-commerce, banking, public utility services and all sorts of on-line ICT-enabled services.

2.2 Objectives

2.2.1 In order to give a thrust to the ICT sector and expeditious development of Software industry and its export required infrastructural facilities and legal framework will be created..

2.2.2 Provide effective incentives for development of ICT sector to both local and foreign entrepreneurs;

2.2.3 Develop an efficient ICT infrastructure that provides open access to international and national network;

2.2.4 Promote and facilitate use of ICT in all sectors of the economy for transparency, good governance and efficiency improvement;

2.2.5 Establish legislative and regulatory framework for ICT issues like IPR, data security and protection, digital signature, e-Commerce, ICT education etc. as well as to ensure quality ICT education provided by different private organizations

2.2.6 Set up national databases that is reliable and easily accessible to all the people of the country;

2.2.7 Promote use of ICT by providing special allocations for ICT project implementation in the public sector. Train the decision makers in ICT use and promote an ICT

2.2.8 Develop a large pool of world class ICT professionals to meet the needs of local and global markets

2.2.9 Set up a very high quality ICT institution to continuously promote and foster ICT Industry;

2.2.10 Enact Laws and Regulations for uninterrupted growth of ICT, in conformity with World Trade Organization (WTO) stipulations

3.0 Policy Statements

3.1 Training and Human Resources Development

Bangladesh must prepare itself to compete effectively in the global ICT market. As the demand for skilled manpower in ICT is growing world-wide, the country needs to produce a large number of ICT professionals. The specific policy statements are:

3.1.1 Widespread introduction of ICT education in public and private educational institutions is a prerequisite for producing skilled ICT manpower. Facilities shall be built to promote ICT training and computer aided training at all levels of education including

Primary Schools and Madrasahs. Donor agencies, non-government organizations and other development partners of the country shall be encouraged to help build the necessary capacity in this area.

3.1.2 Universities, Bangladesh Institutes of Technology and colleges, both in the public and private sectors, shall be strengthened to produce ICT graduates in four-year Computer Science and/or Engineering courses. Necessary resources will be allocated to these institutions.

3.1.3 Out of the three Science and Technology universities proposed in the Fifth Five-Year Plan, one will be established as center of excellence in ICT by giving higher allocation of resources.

3.1.4 Establish multimedia institutes up to district level to start with to produce skilled human resources to exploit the opportunity offered by the growing multimedia-market.

3.1.5 Diploma and Trade Certificate in ICT will be offered in both public and private institutes including Polytechnics. The continual skill upgrading of existing professionals working in public and private sectors shall be ensured by in-service training programmes.

3.1.6 The shortage of trained and qualified teachers and trainers for ICT training is a bottleneck to the HRD plan. To address the issue, IT-Capacity-Building of the Teachers Training Institutes (TTI) including TTCs, NAPE, PTI will be taken up. To teach the teachers and trainers, intensive post-graduate diploma courses will be introduced in TTIs. Training programmes to train and retrain them periodically to keep them up-to-date with the technological progress in the area of ICT will be introduced. ICT literacy will be a desirable requirement in the recruitment and selection of teachers. Divisional training centers of BCC will provide TOT (Training for the Trainers) to build up sufficient number of skilled trainers.

3.1.7 As it would be difficult to train teachers in ICT in large number using the present infrastructure, deploy virtual ICT trainers wherever possible. CD and web based courseware development and use shall be encouraged to promote computer-aided education at all level of education.

3.1.8 To address the issue of deficiency in English and mathematics education, a crash programme shall be taken up to train teachers. To ensure standard and quality of ICT education, a national

certification and accreditation system shall be developed and implemented.

3.1.9 Take up programmes to develop quality ICT professionals and skilled personnel to ensure success in the global software and ICT-enabled services market. Encourage and support formal and informal sector to adopt internationally accepted standards in training programs and to introduce globally acceptable standards.

3.1.10 Use the potential of ICT for delivery of distance education to help stretch the country's limited teaching resources and ensure quality education to all.

3.1.11 Qualified and skilled teachers will be brought in from abroad in the fields where local teachers are not available.

3.1.12 Syllabus and Course Curricula for all levels of Computer Science training will be updated continuously.

3.2 ICT Infrastructure

3.2.1 To ensure capacity building of the nation in the field of Information Technology and to attain a sustainable growth of the ICT sector of Bangladesh and to help compete in the expanding global ICT market, Ministry of Science and Information & Communication Technology and BCC should be appropriately strengthened.

3.2.2 To support the growing demand of the ICT sector, appropriate ICT infrastructure to be established immediately both in public and private sector. As telecommunication infrastructure is an integral part of ICT, so the telecommunication sector should be deregulated and made open to private sector investors as early as possible.

3.2.3 In order to establish direct connectivity with international information and communication backbone Bangladesh will join Fiber Optic Submarine Cable network.

3.2.4 Development of telecommunication infrastructure should be considered as Infrastructure Development Industries like Development of Road, Electricity, Power, Computer/ICT Industry etc.

3.2.5. Facilitate development of telecommunication infrastructure at the least possible cost with little or no customs duty during construction of the infrastructure up to June , 2006.

3.2.6 As telecommunication infrastructure [Telephone Exchange, Towers, Radio/Telephone Transmission Lines etc.] are

similar to electric power infrastructure [Generator, Pylons, Power Grid and Gas Transmission Lines], so Customs Duty & Tax etc. should be amended accordingly in the same line.

3.2.7 Cellular telephone handsets are being increasingly used as terminals for emailing and other ICT uses. Customs duty & tax etc. of cellular mobile telephone handsets should be brought down to a reasonable level.

3.2.8 The use of ICT and information services should be affordable to the people; and therefore the cost (and hence the price) of carriage. Infrastructure & Services should be provided by a multiplicity of enterprises like the BTTB, Railways, Electricity and Gas Companies.

3.2.9 Bangladesh Telegraph and Telephone Board (BTTB) have resources like land, MW/UHF Towers all over the country which should be shared with other Private sector companies for augmenting Information Infrastructure. BTRC should take the leadership to coordinate the activities of Public Utility sectors [BTTB, PDB, Gas, Railway etc.] and make their existing dormant/underutilized infrastructure and resources (land, Microware/UHF Towers building, Radio Towers, Power Pylons, Cable Duct etc.) for the promotion of ICT. BTRC should encourage cooperation between BTTB, Railways, PDB, REB Power Grid Company, Oil and Gas Companies, etc., which have right of way and infrastructure to build digital microwave and optical fiber based photonic information transport systems for use by ICT service providers.

3.2.9 BTTB should cooperate with Private Licensed ICT service providers to transform its underutilized resources into countrywide Information Infrastructure on commercial basis To this end, BTTB should make joint venture agreements with Private Licensed ICT service providers where BTTB will make available its resources like land, Microware/UHF Towers, Cable Duct etc. on a commercial basis under existing rules and practice. The Licensed Private ICT service providers shall provide necessary finance and technology to construct countrywide National Information Infrastructure (NII) for use of all Telecommunication and Internet Service Providers (ISP).

3.2.10 BTTB will increasingly shift its role from Service Provider to individual subscribers Infrastructure Provider to all other Telecommunication Service Providers and ISPs on commercial basis.

3.2.11 Socio-economic development can be accelerated if more people can have access to information. Tele-density is important in this respect and it will be increased to broaden the coverage, which will improve the socio-economic condition of the people through ICT-related activities in line with experience of developed countries.

3.2.12 Basic telecommunication facilities will be extended to the rural and under-served areas to bring the greater mass into the stream of ICT activities both by the public and private sector.

3.2.13 Advanced and new technologies will be introduced to expand the existing network and will be extended gradually to the rural and under served areas.

3.2.14 Telecommunication facility will be made available to all segments of the society and all of the present and emerging services will be provided at an affordable cost.

3.2.15 To provide dial-up Internet access from local telephone calls ISPs will be provided with relevant technological facilities

3.2.16 The Internet facility will be extended to all the district headquarters and subsequently to its adjacent areas up to Upazila levels. Internet will be provided to the educational institutions and libraries.

3.2.17 To ensure public access to information, Cyber Kiosks will be set up in all Post offices, Union complex and Upazila complex. Private sector participation will be encouraged to set up these facilities.

3.2.18 To support the installation of ISPs in the country national high speed communication backbone for Internet will be developed and international high-speed gateway facilities for ISPs will be provided on commercial basis.

3.2.19 Inter-ISP communication is time consuming and costly as there is no Internet exchange in the country at present. The problem will be solved by establishing Internet exchange.

3.2.20 An integrated flexible and reliable nation-wide information communication network capable of voice, audio, video data and graphics transmission will be ensured. National Information Infrastructure will be developed and it will be directly connected to Global Information Infrastructure through Information superhighway to create, collect and sell software and provide ICT enabled services to the world-market through involvement of both the public and private sectors.

3.2.21 To improve the quality of present telecommunication services and to help provide value added services analog telephone-switches and transmission link of the existing telephone network will be replaced by digital switches and digital transmission link as early as possible.

3.2.22 The bandwidth capacity and availability will be ensured all over the country at a reasonable cost to encourage the growth of Internet, ICT industries, e-Commerce and e-Government

3.2.23 Development of local technological capabilities through local ICT industry will be emphasized. The service component of the ICT industry will be conducted by local private firms, in association with foreign firms as and where possible.

3.2.24 Hi-Tech Zones will be established through technology transfer with the cooperation of foreign companies and Bangladeshis working abroad. Software Technology Park with dedicated and advanced data communication facilities shall be established and software development and export companies will be encouraged to set up workspace in those parks at preferential terms.

3.2.25 A central depository for collection and dissemination of ICT information and research findings will be developed. This will be done under a network, connecting all university libraries and research organization to this central depository, which in turn will be connected to the Internet.

3.2.26 Solar power will be encouraged specially in those inaccessible areas where use of ICT is constrained due to lack of electricity

3.2.27 Use of VoIP and WLL (Wireless Local Loop) technologies will be reviewed and realistic measures taken thereafter.

3.3 Research and Development in ICT

3.3.1 Research and development in ICT will focus on need based fundamental and applied research contributing to the improvement of quality and efficiency of the application to our ICT industry.

3.3.2 Bangladesh Computer Council will encourage ICT R&D activities carried out by the public and private sector organisations.

3.3.3 BCC along with ICT industries will assist in formulating plans to conduct need-based R&D activities in the Universities, BITs and public & private sector R&D institutions and encourage the younger generation in these activities. The ICT industry may fund for R&D activities for new ICT products and services through Industry-Academia collaboration.

3.3.4 A central on-line data bank for scientific and technological information will be established which can be accessed by educational institutions and other R&D organisations.

3.3.5 R&D efforts on Bangla text processing, Bangla voice recognition, translation and synthesis will be intensified.

3.3.6 Technology Corporations such as Microsoft, IBM, Computer Associates, Oracle, SAP etc. will be approached to set up their R & D Centers in Bangladesh.

3.3.7 Contents for Internet and Intranet will be developed in Bangla

3.4 ICT Industry

3.4.1 Software Industry

3.4.1.1 To develop and encourage the local software industry, price preference may be given to locally developed software in all public and private sector procurement.

3.4.1.2 In order to assist fast development of local Software Industries, Government will set up an ICT Incubator. The government will extend start-up financial support to the local software industry. Non-Resident Bangladeshis and experts will be encouraged to set up software development companies.

3.4.1.3 The associations of software companies and developers should be encouraged to exchange ideas, experience and organize collective operations such as seminars, training, etc. and take part in trade delegations and trade shows for acquaintance with the international market, trends and establishment of business contacts.

3.4.1.4 The Export Promotion Bureau (EPB) and Commercial wing of Bangladesh Missions abroad shall take vigorous steps to identify and explore markets for export of software, data entry services and ICT-enabled services from Bangladesh, including promotion of strategic partnership and outsourcing opportunities.

3.4.1.5 Joint ventures between local and foreign entrepreneurs in the ICT sector will be vigorously promoted.

3.4.1.6 An annual target of 3 (three) billion US dollars from earnings of export of software, data entry and IT-enabled services shall be planned up to year 2006. The target shall be revised periodically to match the growth of the market.

3.4.2 Hardware Industry

3.4.2.1 Hardware industry often requires a huge capital investment and entrepreneurs shall be encouraged to establish production facilities for components, peripherals and accessories with joint venture cooperation and technology transfer agreements. Foreign owned and multinational companies, who will establish such production facilities in Bangladesh and employ our workforce, shall be offered special incentives.

3.4.2.2 IT/ICT Laboratories and resource center in universities and other concerned institutions will be set up to develop skilled manpower required to establish and run hardware industry.

3.4.2.3 Since the local market is still small, the hardware industry may target the export market. Dependence on foreign materials should be reduced where possible by giving incentives to local companies and protecting them from unfavorable competition. Local institutions and R&D organizations shall also be encouraged for research, design, and manufacturing of specialized informatics equipment.

3.4.3 Services Industry

3.4.3.1 Bangladesh, having the advantage of cost-effective labour, must endeavor for expansion and export of ICT-enabled services such as medical transcription, data entry, data processing, call centers etc. at home and abroad.

3.4.3.2 NGOs interested to contribute for the expansion of ICT sector, will be provided with facilities.

3.5 E-Commerce

3.5.1 The Government and the private sector will promote business in electronic form and create an environment in which it will be well secured. Government will take initiative to introduce and

promote Government-to-Government (G2G) transaction under the purview of e-commerce. Gradually this initiative will also be extended from G2G to Government to Business (G2B) transaction in the same line.

3.5.2 Authentication of the identities of both buyer and seller or the involved parties in an electronic transaction is crucial to promote inter-bank transaction, encryption e-commerce. Security of electronic transaction should be ensured through appropriate measures.

3.5.3 Establish immediately inter-banking payment system in electronic form.

3.5.4 Legal framework to provide the guiding principles, rules and legislation for e-Commerce shall be put in place.

3.6 e-Government / e-Governance

3.6.1 The Government shall use ICT system within the public administration to improve efficiency, reduce wastage of resources, enhance planning and raise the quality of services.

3.6.2 Government shall implement wide-spread ICT systems to provide nation wide coverage and access by any citizen to the government databases and administrative systems which can be used to extend public services to the remotest corner.

3.6.3 All Government ministries, divisions, departments, autonomous bodies and all District headquarters, Upazilla headquarters and Union Porishad offices must be networked to the National Data Resource Centre in the shortest possible time. The centre shall be a system of national databases having capacity to store and supply rapidly all necessary information on the economic, cultural and social situation of our country.

3.6.4 Each Ministry, Division, Government body shall create a ICT Cell, to be managed and run by well trained ICT professionals to plan, coordinate and implement ICT projects and services. Special compensation package comparable to that of private sector shall be introduced to encourage ICT professionals.

3.6.5 All Ministries, Divisions, agencies of government and autonomous organizations shall set up web sites where all policy documents and information relevant to the public shall be posted as early as possible and regularly updated. There will be a web portal of Bangladesh Government from which link will be provided to the web sites, like e-forms, e-procurement, e-recruitment, e-results etc.

3.6.6 Government will introduce and promote ICT based services like G2G (Government to Government), G2E (Government to Employee), G2C (Government to Customer) etc.

3.6.7 Preference shall be given to ICT literate candidates for the purpose of recruitment in public offices. ICT-literacy shall also be evaluated in the ACR of officials to ensure utilization of ICT in the public services.

3.6.8 In order to establish database on the secondary schools which are providing computers training at grass root level, MIS will be introduced.

3.7 Legal Issues

3.7.1 Software copyright provisions embodied in the Copyright Act 2000 will be implemented by promptly setting up appropriate enforcing bodies as mentioned in the Act.

3.7.2 ICT Act should be enacted immediately to protect against computer crimes such as computer fraud, hacking and damage to programs and data and introducing/spreading computer viruses.

3.7.3 Data security and interoperability should be ensured through actions such as setting of encryption standards and international agreements on interoperability.

3.7.4 With the increase in the use of Internet and Information Technology in every sphere of human activities, formulation of new laws or amendment to the existing ones should be done as deemed necessary, to ensure security of data, freedom of information.

3.7.5 ICT will be used by the law enforcing agencies to ensure safety and security of life and property of the citizen.

3.7.6 Agencies like Police, NBR and BAC shall use ICT for quick disposal and monitoring of investigation of cases.

3.7.7 Bangladesh Armed forces should use ICT to the fullest extent to increase their efficiency and effectiveness.

3.8 Health Care

3.8.1 The main focus in the use of ICT and communication technologies in Healthcare will be to deliver new capabilities for hospitals and healthcare providers. ICT should be used to develop such capabilities specifically in the areas of electronic medical records, telemedicine, medical and health education, etc.

3.10.3 Non-government organizations will be encouraged to establish centers at the village level for providing hardware/software or other support services. At the same time the Government will use both the formal and non-formal channels to disseminate information about the application, advantages to communities of the use of ICT.

3.11 Transportation

3.11.1 The government will introduce an ICT-based integrated transport management system.

3.11.2 Commercial transport agencies will be encouraged to deploy Information Technology for dynamic route planning and traffic management.

3.11.3 ICT will be used for online booking and ticketing services of all public and private transport companies.

3.12 Tourism: To harness the potential of the tourism industry in Bangladesh, Information Technology should be strengthened aggressively:

3.12.1 Information Technology should be used to project tourists' attractions in Bangladesh through the Internet.

3.12.2 A reliable, comprehensive, on-line information system to satisfy the needs of the tourists for travel and accommodation to deliver instant and up-to-date information will be developed.

3.12.3 The partnership with both the local and foreign agencies relevant to tourism will be strengthened and encouraged to introduce on-line reservation for travel and accommodation, booking and ticketing for arts and entertainment events and shopping.

3.13 Environment: The growing environmental pollution has endangered all forms of lives including the human existence. In this era of wired world, the Information Technology can help build the capabilities to fight against the environmental degradation.

3.13.1 Information Technology will be deployed to collect and disseminate information on environmental problems and their causes in order to create awareness about environment among the common people.

3.13.2 Information system for making a complete inventory of existing flora & fauna of Bangladesh, their habitats and other natural communities whose existence has been endangered will be created.

3.8.2 Telemedicine System Network shall be introduced throughout the country for cost-effective delivery of health care services. The Telemedicine Network will be used for rural patient management, distant medical education, training of health professionals and to develop mass awareness for disease prevention.

3.8.3 Development of Bangladesh Health Portal should be given priority for appropriate growth of e-health and telemedicine referral system. International tele-consultation through telemedicine for critical patients will be promoted in both private and public sector.

3.8.4 All public hospitals and medical research centers shall be linked by computer networks with Medical center of excellence as the central hub in order to make expert services available throughout the country. This network may be gradually extended to the local level.

3.9 Agriculture and Poverty Alleviation

3.9.1 Agriculture including fisheries and livestock is the main source of earnings for the majority of the people of Bangladesh and hence use of ICT systems in these sectors are very much essential to reap its unutilized potentials and thereby improving the socio economic conditions particularly of the rural people. Proper initiatives will be taken to utilize ICT systems in agro-based industries, agricultural research, and dissemination of agricultural technology, agri-business development to the farmers and preparation and maintenance of agricultural database.

3.10 Social Welfare

3.10.1 Nation-wide ICT systems will be implemented for rural development activities, agricultural, horticulture, fisheries and livestock extension for farmers, career guidance for youth, technology guidance for rural enterprises, micro level planning etc. Communities and user groups or beneficiaries would be actively encouraged to participate in all such activities.

3.10.2 Public grievance redressal will be incorporated in the ICT-based system to facilitate access to citizens through any of the kiosks, public facilitation centers or Government offices. It would be made email based and strengthened to facilitate monitoring and on-line responses.

3.10.3 Non-government organizations will be encouraged to establish centers at the village level for providing hardware/software or other support services. At the same time the Government will use both the formal and non-formal channels to disseminate information about the application, advantages to communities of the use of ICT.

3.11 Transportation

3.11.1 The government will introduce an ICT-based integrated transport management system.

3.11.2 Commercial transport agencies will be encouraged to deploy Information Technology for dynamic route planning and traffic management.

3.11.3 ICT will be used for online booking and ticketing services of all public and private transport companies.

3.12 **Tourism:** To harness the potential of the tourism industry in Bangladesh, Information Technology should be strengthened aggressively:

3.12.1 Information Technology should be used to project tourists' attractions in Bangladesh through the Internet.

3.12.2 A reliable, comprehensive, on-line information system to satisfy the needs of the tourists for travel and accommodation to deliver instant and up-to-date information will be developed.

3.12.3 The partnership with both the local and foreign agencies relevant to tourism will be strengthened and encouraged to introduce on-line reservation for travel and accommodation, booking and ticketing for arts and entertainment events and shopping.

3.13 **Environment:** The growing environmental pollution has endangered all forms of lives including the human existence. In this era of wired world, the Information Technology can help build the capabilities to fight against the environmental degradation.

3.13.1 Information Technology will be deployed to collect and disseminate information on environmental problems and their causes in order to create awareness about environment among the common people.

3.13.2 Information system for making a complete inventory of existing flora & fauna of Bangladesh, their habitats and other natural communities whose existence has been endangered will be created.

3.13.3 GIS and other ICT-based systems will be set up for planning at the national level, for agricultural crops estimation, for conservation of nature while accommodating compatible land use to maintain the ecological balance.

3.13.4 Information and Communication Technology will be used to help solve the most pressing problems of environment in the urban areas like toxic emissions from vehicles, industries and other sources.

3.14 Judiciary

3.14.1 To enhance the capacity of the judiciary, computer based Management Information System (CMIS), with suitable Wide Area Network (WAN) and Local Area Network (LAN), will be established for the Supreme Court and for the District Courts and Tribunals. It may consists of three inter-related modules, namely, (i) a case management module, (ii) a legal framework module, essentially covering two basic sources of updates, namely the Bangladesh legislative code and the Bangladesh case law (reported Supreme Court rulings) database and (iii) a court administration module, whose areas of application may include court inspection, planning and budgeting, transactions, financial accounts, staff-related information and reporting, statistical applications and records management.

3.15 Regional and International Cooperation

3.15.1 The Ministry of Science and Information & Communication Technology and BCC will be the focal point for the regional and international cooperation in the area of Information and Communication Technology.

3.15.2 The Ministry of Science and ICT shall explore Regional, Sub-Regional and International cooperation and execute collaborative agreements on ICT with developed and developing countries as well as with relevant international agencies and development partners.

3.15.3 The Ministry of Science and ICT will facilitate participation in the regional and international forum to reap benefit for the country's economy.

4.0 Implementation and Monitoring

4.1 Funds and Resources

4.1.1 Government spending in ICT shall be increased to at least 2% of ADP by 2006.

4.1.2 New budget provision for ICT should be created for all Ministries, Divisions, Departments and Bodies and all Autonomous sectors should be encouraged to make their own investment in the application of ICT in production, trade and services. ERD should explore external assistance for necessary infrastructure and human resources development conforming to the ICT Policy.

4.1.3 Those ICT companies will get preferential terms, which will be able to meet up 20 percent of its revenue expenditure from the earnings of export of software and ICT-enabled services.

4.1.4 A centralized fund for R&D and HRD will be created within BCC. It will be encouraged to contribute 1% of all profits from Software and ICT-enabled services to the R&D and HRD fund.

4.2 Institutional Arrangement for ICT Policy Updating, Standardizing, Implementing and Monitoring

4.2.1 In order to make best utilization of ICT and exploit its immense potential in the economic, social, commercial, and scientific fields, a National ICT Task Force headed by the Hon'ble Prime Minister has already been formed. This apex national body will guide in updating, standardizing, implementing, and monitoring the ICT policy.

4.2.2 The Ministry of Science and Information & Communication Technology will collaborate with all Ministries /Divisions / Departments / Autonomous Bodies including Banks and Insurances to promote and use ICT in respective areas of operation.

4.2.3 MOSICT shall remain alert and apprise the Government on the progress and development of ICT sector both at home and abroad.

4.2.4 MOSICT will work in unison with the private sector and Universities as promoter of ICT activities and business.

4.2.5 MOSICT and BCC will be reorganized and strengthened in phases to cope with the present need and future requirement of ICT.

ABBREVIATIONS & ACRONYMS

ADP	Annual Development Program
BAC	Bureau of Anti-Corruption
BCC	Bangladesh Computer Council
BIT	Bangladesh Institute of Technology
BTTB	Bangladesh Telegraph and Telephone Board
CD	Compact Disc
ERD	Economic Relations Division
GIS	Geographic Information System
HRD	Human Resource Development
ICT	Information and Communication Technology IT Information Technology
MOSICT	Ministry of Science and Information & Communication Technology
MW	Micro Wave
NAPE	National Academy for Primary Education
NBR	National Board of Revenue
NII	National Information Infrastructure
PDB	Power Development Board
PTI	Primary Teachers Training Institute
R&D	Research and Development
REB	Rural Electrification Board
TTC	Teachers Training College
UHF	Value Added Tax
WAN	Wide Area Network

THE (INDIAN) INFORMATION TECHNOLOGY ACT 2000 (No. 21 OF 2000)

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyaistha 19, 1922 *(Saka)*

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—

[*9th June*, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:–

CHAPTER I
PRELIMINARY

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to, —

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;

(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;

(d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

(e) any contract for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2. Definitions

(1) In this Act, unless the context otherwise requires,–

(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;

(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,–

(i) Enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a license to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, 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;

(j) "computer network" means the interconnection of one or more computers through–

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators

which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media,punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under subsection (4) of section 35;

(r) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, byelaws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that–

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether–

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II
DIGITAL SIGNATURE

3. Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known' as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III
ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.

Where any law provides that information or any other matter shall be in writing or in the type written or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signatures.

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied,) if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies.

(1) Where any law provides for–

(a) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is affected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe–

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

7. Retention of electronic records.

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if–

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette.

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette: Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature.

The Central Government may, for the purposes of this Act, by rules, prescribe–

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

CHAPTER IV
ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.

An electronic record shall be attributed to the originator–

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt.

(1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by–

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:–

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,–

(i) receipt occurs at the time when the electronic, record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer

resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section,–

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

CHAPTER V
SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

14. Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was–

(a) unique to the subscriber affixing it;
(b) capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including–

(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.

CHAPTER VI
REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.

The Controller may perform all or any of the following functions, namely: –

(a) exercising supervision over the activities of the Certifying Authorities;
(b) certifying public keys of the Certifying Authorities;
(c) laying down the standards to be maintained by the Certifying Authorities;
(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
(g) specifying the form and content of a Digital Signature Certificate and the key,
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities.

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository.

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall–

(a) make use of hardware, software and procedures that are secure .iJm intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

21. Licence to issue Digital Signature Certificates.

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification,

expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government

(3) A licence granted under this section shall–

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence.

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by–

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence.

An application for renewal of a licence shall be–

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence.

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of licence.

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has, –

(a) ade a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) ailed to comply with the terms and conditions subject to which the licence was granted;

(c) ailed to maintain the standards specified under clause (b) of sub-section (2) of section 20;

(d) ontravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence: Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him: Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

26. Notice of suspension or revocation of licence.

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories: Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock: Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.

(1)Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person in-charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.

Every Certifying Authority shall, –

(a) ake use of hardware, software and procedures that are secure from intrusion and misuse;

(b) rovide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) dhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) bserve such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of licence.

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure.

(1) Every Certifying Authority shall disclose in the manner specified by regulations–

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall–

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

35. Certifying Authority to issue Digital Signature Certificate.

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government

(2) Every such application shall be accompanied by such fee not exceeding twenty five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under subsection (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application: Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant: Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate.

A Certifying Authority while issuing a Digital Signature Certificate shall certify that--

(a) it has complied with the provisions of this Act and the rules and regulations made there under,

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair,

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to(d).

37. Suspension of Digital Signature Certificate.

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate, –

(a) on receipt of a request to that effect from–

(i) the subscriber listed in toe Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber,

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it–

(a) where the subscriber or any other person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that–

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has bee given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation.

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

CHAPTER VIII
DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate–

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that–

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX
PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, –

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base 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 any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised 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 thereunder;

(h) 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, he shall .be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,–

(i) "computer contaminant" means any set of computer instructions that are designed–

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to–

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate.

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer' for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and–

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

47. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely: –

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default

CHAPTER X
THE CYBER REGULATIONS APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government

50: Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he–

(a) is, or has been. or is qualified to be, a Judge of a High Court; or

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement

benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office: Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal.

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of tony-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of tony-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to" the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal.

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a ·suit, in respect of the following matters, namely: –

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it *ex pane;*

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation.

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction.

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order. Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions.

(1) Any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.—For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be,

shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI
OFFENCES

65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its 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, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

68. Power of Controller to give directions.

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a Fine not exceeding two lakh rupees or to both.

69. Directions of Controller to a subscriber to extend facilities to decrypt information.

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

70. Protected system.

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars.

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that–

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention committed outside India.

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments.

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAPTER XII
NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. Network service providers not to be liable in certain cases.

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section, –

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

CHAPTER XIII
MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have overriding effect.

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

82. Controller, Deputy Controller and Assistant Controllers to be public servants.

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

83. Power to give directions.

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith.

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

85. Offences by companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall

be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section, –

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

86. Removal of difficulties.

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty: Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules.

(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following mailers, namely: –

(a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(b) the electronic form in which filing, issue, grants or payment shall be affected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of .payment under sub-section (2) of section 6;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;

(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;

(g) other standards to be observed by the Controller under clause (b) of subsection (2) of section 20;

(h) the requirements which an applicant must fulfil under sub-section (2) of section 21;

(i) the period of validity of licence granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for licence may be made under sub-section (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for licence under clause (a) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a licence and the fee payable there of under section 23;

(n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(p) the manner in which the adjudicating officer shall hold inquiry under subsection (1) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

(r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;

(t) the salary and allowances and other conditions of service of other officers and employees under sub-section (3} of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub -section (3) of section 57;

(v) any other power of a civil court required to be prescribed under clause (g) of subsection (2) of section 58; and

(w) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Central Government under clause (f) of subsection (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee.

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise–

session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or he of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under (hat regulation.

90. Power of State Government to make rules.

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely: –

(a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6;

(c) any other matter which is required to be provided by rules by the State Government.

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860.

The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

92. Amendment of Act 1 of 1872.

The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

93. Amendment of Act 18 of 1891.

The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1834.

The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

THE FIRST SCHEDULE

(See section 91)

AMENDMENTS TO THE INDIAN PENAL CODE

(45 OF 1860)

1. After section 29, the following section shall be inserted, namely:—

Electronic record.

"29A. The words "electronic record" shall have the meaning assigned to them in clause (t) of subsection

(1) of section 2 of the Information Technology Act, 2000.".

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 464,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely:—

"A person is said to make a false document or false electronic record–

First—Who dishonestly or fraudulently–

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration. ";

(b) after Explanation 2, the following Explanation shall be inserted at the end, namely:–

'Explanation 3.—For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause (d) of subsection (1) of section 2 of the Information Technology Act, 2000.'.

10. In section 466,–

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;

(b) the following Explanation shall be inserted at the end, namely:–

'Explanation.—For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of subsection (1) of section 2 of the Information Technology Act, 2000.'.

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely: —

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.".

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

THE SECOND SCHEDULE

(*See* section 92)

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872 (1 OF 1872)

1. In section 3,—

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely:— 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'.

2. In section 17, for the words "oral or documentary,", the words "oral or documentary or contained in electronic form" shall be substituted.

3. After section 22, the following section shall be inserted, namely:—

When oral admission as to contents of electronic records are relevant.

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.".

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely:—

What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.".

7. After section 47, the following section shall be inserted, namely:—

Opinion as to digital signature where relevant.

"47A. When the Court has 10 forms an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.".

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely:—

Special provisions as to evidence relating to electronic record.

'65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

Admissibility of electronic records.

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: —

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period

or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

1. After section 67, the following section shall be inserted, namely:–

Proof as to digital signature.

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

11. After section 73, the following section shall be inserted, namely:—

Proof as to verification of digital signature.

'73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct–

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation.—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000'.

12. Presumption as to Gazettes in electronic forms.

After section 81, the following section shall be inserted, namely: —

"81 A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.".

shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, —

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, —

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with

or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

1. After section 67, the following section shall be inserted, namely:–

Proof as to digital signature.

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

11. After section 73, the following section shall be inserted, namely:—

Proof as to verification of digital signature.

'73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct–

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation.—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000'.

12. Presumption as to Gazettes in electronic forms.

After section 81, the following section shall be inserted, namely: —

"81 A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.".

13. Presumption as to electronic agreements.

After section 85, the following sections shall be inserted, namely:—

"85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

Presumption as to electronic records and digital signatures.

85B. (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Presumption as to Digital Signature Certificates.

85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.".

14. Presumption as to electronic messages.

After section 88, the following section shall be inserted, namely:—

'88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.'.

15. Presumption as to electronic records five years old.

After section 90, the following section shall be inserted, namely: —

"90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation.—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to section 81A.".

16. For section 131, the following section shall be substituted, namely: —

Production of documents or electronic records which another person, having possession, could refuse to produce.

"131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.".

THE THIRD SCHEDULE

(See section 93)

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT ' 1891 (18 OF 1891)

1. In section 2—

(a) for clause (3), the following clause shall be substituted, namely:—

'(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

(b) for clause (8), the following clause shall be substituted, namely: — '(8) "certified copy" means when the books of a bank,

(a) are maintained in written form, a copy of any entry in such books together with a certificate written;:: the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'.

1. After section 2, the following section shall be inserted, namely:— .

Conditions in the printout.

"2A. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of–

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F} the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.".

THE FOURTH SCHEDULE

(See section 94)

AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934 (2 OF 1934)

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely:—

"(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-I, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;".

SUBHASH C. JAIN,

Secy. to the Govt. of India.

PRINTED BY THE MANAGER, GOVERNMENT OF INDIA PRESS (PLU), MINTO ROAD, NEW DELHI AND PUBLISHED BY THE CONTROLLER OF PUBLICATIONS, DELHI, 2000.

MGIP(PLU)MRND—1359G1—14-6-2000.

Chapter 34

UNCITRAL Model Law on Economic Commerce United Nations Commission on International Trade Law (UNCITRAL)

Objectives

The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly and is expected to develop further as technical supports such as information highways and the Internet become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity.

The purpose of the UNCITRAL Model Law on E-Commerce is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce". The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce.

The decision by United Nations Commission on International Trade Law (UNCITRAL) to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate because it does not contemplate the use of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents.

While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may result in

uncertainty as to the legal nature and validity of information presented in any form other than a traditional paper document. Moreover, while sound laws and practices are necessary in all countries where the use of EDI and electronic mail is becoming widespread, this need is also felt in many countries with respect to such communication techniques as telecopy and telex.

The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques.

Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions that create legal obstacles to the use of electronic commerce. As between those States, which are parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce.

The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade.

Scope

The title of the Model Law refers to "electronic commerce". While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce".

Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the Internet. In certain circumstances, the notion of "electronic

commerce" might cover the use of techniques such as telex and telecopy.

It should be noted that, while the Model Law was drafted with constant reference to the more modern communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy.

Such situations are intended to be covered by the Model Law, based on a consideration of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably.

The objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

Depending on the situation in each enacting State, the Model Law could be implemented in various ways, either as a single statute or in several pieces of legislation.

Structure

The Model Law is divided into two parts, one dealing with electronic commerce in general and the other one dealing with electronic commerce in specific areas. It should be noted that part two of the Model Law, deals with electronic commerce as it applies to the carriage of goods. Other aspects of electronic commerce might need to be dealt with in the future, and the Model Law can be regarded as an open-ended instrument, to be complemented by future work.

UNCITRAL intends to continue monitoring the technical, legal and commercial developments that underline the Model Law. It might, should it regard it advisable, decide to add new model provisions to the Model Law or modify the existing ones.

A "framework" law to be supplemented by technical regulations The Model Law is intended to provide essential procedures and

principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances. However, it is a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement those techniques in an enacting State. Moreover, the Model Law is not intended to cover every aspect of the use of electronic commerce.

Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law.

The "functional-equivalent" approach

The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication.

The Model Law permits States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements.

The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.

For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts.

It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document. That is why the Model Law adopted a flexible standard.

The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function.

Default rules and mandatory law

The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to most of the legal difficulties raised by the use of modern means of communication are sought within contracts. Chapter III of part one contains a set of rules of the kind that would typically be found in agreements between parties.

Parties may use the rules contained in chapter III of part one as a basis for concluding such agreements. They may also be used to supplement the terms of agreements in cases of gaps or omissions in contractual stipulations. In addition, they may be regarded as setting a basic standard for situations where data messages are exchanged without a previous agreement being entered into by the communicating parties, e.g., in the context of open-networks communications.

The provisions contained in chapter II of part one is of a different nature. One of the main purposes of the Model Law is to facilitate the

use of modern communication techniques and to provide certainty with the use of such techniques where obstacles or uncertainty resulting from statutory provisions could not be avoided by contractual stipulations.

The provisions contained in chapter II may, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy.

The provisions contained in chapter II should be regarded as stating the minimum acceptable form requirement and are, for that reason, of a mandatory nature, unless expressly stated otherwise in those provisions. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

Bangladesh Telecommunications Regulations & Policies

The Telegraph Act No XIII was passed in 1885 & Wireless Telegraphy Act was passed in 1993. The Bangladesh Telecommunication Act No. 18 was passed on April 16 of 2001, setting the scene for a radical change to the regulatory environment. The Telegraph branch under the Posts and Telegraph Dep't was created in 1853 in the then British India, and was regulated after wards under the Telegraph Act of 1885. This was reconstructed in 1962 in Pakistan regime. After independence of Bangladesh in 1971 Bangladesh Telegraph and Telephone Department was set up under the Ministry of Posts and telecommunications (MOPT) to run the Telecommunications Services in Bangladesh. This was converted in to a corporate body namely "Telegraph and Telephone Board by promulgation of Telegraph and Telephone Board ordinance, 1975. Under the provisions of ordinance No. XII of 1979 of 24th February, 1979 Telegraph and Telephone Board was converted into "Bangladesh Telegraph and Telephone Board (Called BTTB) as a government Board. The Bangladesh Telecommunication Regulatory Commission (BTRC) was established on January 31, 2002 under the Government of the People's Republic of Bangladesh By Act no. 18 of 2001, as an Independent Regulatory Commission. The BTRC consists of five appointed Commissioners including Chairman and a Vice-Chairman.

Telecommunication Structure

Government of the People's Republic of Bangladesh
Bangladesh Telecommunication Regulatory Commission
Service Providers (Operators)

Objectives of the Commission:

The following are the objectives of the Commission:-
Issue license to operators
Managing of he radio frequency spectrum
Arranging of spectrum monitoring
Prepare the national numbering plans & signaling point code

Dispute re-solution

Control tariffs.

Regulate technical standards

Investigating complaints against licensed operators.

Represent in international telecommunication organization.

Encourage investment in telecommunication sector.

Promoting effective competition in the telecommunication sector.

ICT/IT Policy

* Bangladesh has an ICT Policy

* The vision of the policy:

* This Policy aims at building an ICT-driven nation comprising of knowledge based society by the year 2006. In view of this, a country wide ICT-infrastructure will be developed to ensure access to information by every citizen to facilitate empowerment of people and enhance democratic values and norms for sustainable economic development by using the infrastructure for human resources development, e-governance, e-commerce, banking, public utility services and all sorts of on line ICT-enabled services.

* It has been formulated by the Ministry of Science and Information & Communication Technology.

Next Generation Network

Bangladesh Telecommunication Regulatory Commission (BTRC) is responsible to make regulation to introduce Next Generation Network and Service in Bangladesh.

The Regulation is now on process.

BTRC is intending to provide 3G IP based WLL technologies to covert the country.

Nationwide Network Architecture

- In order to establish direct connectivity with International Information and Communication Backbone Bangladesh will join Fiber Optics Submarine Cable Network. The Project is

going on and at the end of 2005 we will be the member of Submarine Cable Network.

- BTTB has installed fiber optics backbone network throughout the country with a microwave backup in some portion.
- Grameen Phone is now using the optical fiber of Bangladesh Railway as a lease basis. They also make sublease to other DDCSP and ISP's.
- TMIB, PBTL and Sheba Telecom Limited (Mobile Operators) have installed Microwave backbone in different areas of the Country.
- Power Grid Company of Bangladesh (PGCB) is going to install an optical fiber network along with their high voltage line. They are also interested to lease it to the telecom and data operators licensing by BTRC is in the process.
- GTCL is going to install an optical fiber network along with their gas pipe line. They are interacted to lease it to the telecom and data operators.

Technology

- Four Mobile operators are using GSM Technology and one Mobile operator is using CDMA Technology in Bangladesh.
- Most of the ISP's are using dialup, cable modem, wireless technology to provide service.
- All the DDCSP's are using Wireless technology (License Frequency) to provide service.
- BTRC is processing to reduce the price in the affordable and reliable level for interconnection.

Main Issues before BTRC

- Interconnection
- Licensing
- Tariff
- Dispute Resolution
- Managing of the Radio Frequency Spectrum

- Spectrum Monitoring
- Allocation of Numbering Plans & Signaling Point code
- Technical Standardization
- Technical Standardization
- VOIP WLL BE OPENED VERY SOON. Now license conditions are being determined by BTRC

AN INTRODUCTION OF THE BANGLADESH TELECOMMUNICATION REGULATORY COMMISSION

(BTRC) Presented By

Justice Mohammad Abdus Salam , Commissioner
Bangladesh Telecommunication Regulatory Commission

CONTENTS

A. Bangladesh Scenario in telecom. Sector:-

Bangladesh with an area of 1,44,000 sq. kilometers has currently more than 144 million populations. Dhaka its capital city with 12 million residents have high demand for telecom services; the other metropolitan cities such as Chittagong, Sylhet, Khulna, Rajshahi and Barisal have proportionately higher demand for telephone service as compared to the rest 56 district towns. The 460 thana headquarters and other commercially advanced places in the rural areas have also demand for telephone services which all need to be brought under a well developed broad based nationwide network of telephone service with easy access and connectivity with the global telecommunication system.

Fixed telephone with analogous, digital, NWD, ISD, Cellular mobile phone, internet service for data communication, VSAT services are already operating in Bangladesh. BTTB is main player providing fixed phone services. 4 mobile phone services Operators in partnership with foreign investors are providing GSM phone services some local

and foreign companies are already in the race to operate PSTN service in the rural areas. Mobile phone service through satellite are also on way of introducing service in Bangladesh. BTTB as the state owned largest operator is providing the major services and is taking initiatives to expand the areas under its service network, fixed and mobile phone service. Approximately there are 9 lacs fixed telephone subscribers and 7 millions mobile phone subscribers. On the commencement of the Bangladesh Telecommunication Act, 2001 BTTB became and operator like other private operators and has to be corporatise within one year. Teledensity in Bangladesh is 4.58%.

B. National Telecommunication Policy (NTP): -

Govt. of Bangladesh (GOB) by its National Telecommunication Policy declared in 1998 liberalized the telecommunication sector and opened it for private participation by local and foreign investors.

NTP reflects the commitments of the GOB and thereby aims at a national sound telecommunication Infrastructure to support the economy and welfare of the country by providing telecommunication facilities on demand, assuring satisfactory quality of service in all the areas through equitable opportunity and healthy competitions in level playing field among the service providers.

Under the NTP foreign investors are allowed to invest and own 100% share of their investment individually or on joint venture keeping in with the Industrial policy of the Government on BOT, BOO scheme.

NTP sets the target by 2000 to increase teledensity from 0.4 to 1 for every 100 persons and to 4 telephones for every 100 persons by 2010 including bringing thanas, unions and village under the telecommunication network.

NTP also aims at establishment of Bangladesh

Telecommunication Regulatory Commission with a view to transferring the regulatory functions of the MOPT to the BTRC.

C. Legislations Governing the Telecommunications in Bangladesh: -

The Telegraph Act 1885.

The Wireless Telegraphy Act. 1933

The Bangladesh Telegraph and Telephone Board Ordinance 1979.

The Bangladesh Telecommunication Act 2001.

BTA is the latest legislation under which the BTRC is established with the vesting of certain powers and regulatory functions in Telecom. Sector. This Act of 2001 has superseding and overriding effect over all other laws to the extent they are inconsistent therewith.

D. Salient aspects of the Bangladesh Telecommunications Act 2001 (Act No. 18 of 2001):-

The Bangladesh Telecommunications Act 2001 after its enactment by the Parliament and assented to by the President was published in the Bangladesh Gazette on 16th April 2001 and was subsequently by a Gazette notification put into effect on 31st January 2002.

The Act aims at establishing the BTRC as an independent commission the legislative intent of which has been manifested in the preamble.

The Bangladesh Telecommunication Act 2001 provides for establishment of the BTRC, it's powers and functions, offences and punishment thereunder etc.

E. Composition of the BTRC and tenure of office:-

Pursuant to the provision of section 6 of the Bangladesh Telecommunication Act 2001 the Bangladesh Telecommunication Regulatory Commission (BTRC) was established on 31st January 2002.

As provided under section 7 of the Act BTRC is composed of 5 commissioners appointed by the President for a term of three years with the eligibility of reappointment for another term subject to the age limit of 65 years. Of the Commissioners one is appointed the Chairman and the other as Vice Chairman. A Commissioner may resign his post or he may be removed through enquiry to be held by a committee of judge of the Supreme Court on ground of inefficiency, gross misconduct and corruption.

F. Administrative setup and Organgram:-

For the purpose o carrying out the functions of the Commission there are 5 (five) divisions such as (1) Administration and finance (2) Systems and services (3) Engineering and operation (4) Spectrum Management and (5) Legal and Licensing Organogram:-

G. Functions of the BTRC:-

Functions of the BTRC among others include:-

To regulate establishment, operation and maintenance of telecom services in Bangladesh

To control and abolish discriminatory practice and ensure level playing field for the operators for healthy competition.

To hear and resolve objections, disputes and complains through public hearing and issue injunction and enforcement orders.

H. Powers of the BTRC

BTRC has the exclusive power:-

- to grant license for establishing, operating telecommunication system, providing telecom services, using radio apparatus.
- to issue technical acceptance certificates
- to allocate frequency, monitor and manage spectrum
- to renew, suspend or cancel licnece, permits and certificates
- to approve tariff and call charges among the operators and levy charges.
- to inspect telecom installation and terminal apparatus etc.
- to stop interference caused by one operator to the another's service systems
- to issue permission as to right of way of the operator to his installation
- to frame regulations as to procedure and other aspects for carrying out the purpose of the Act,
- seize illegal equipments and apparatus, arrest the offenders, investigate into the commission of offence by its own officer and submit charge sheet.

I. Offences and punishments under the Act:-

To establish, operate or use radio apparatus and radio frequency and provider telecom service without licence from BTRC constitute offence punishable with imprisonment up to 10 years or and fine up to Taka 10 lacs. offences under the Act are investigated by the officers of the BTRC and not by the Police and exclusively triable by the Court of Session.

BTRC can impose administrative fine up to taka one lac for violation of injunction or enforcement order. If such fine is not paid

this constitutes offence punishable with imprisonment up to 3 years and or fine up to taka 3 lacs.

BTRC can also impose for violation of any provision of law or the conditions of licence or permit or regulation, administrative fine up to taka 3 lacs 30 thousand for each day continuing violation.

J. Regulatory decision making and procedure:-

Regulatory decision making involves adjudicatory process when it relates to dispute resolution and complaints.

Norms and procedure of regulatory decision are different from that of the court proceedings of adversarial nature where full dress trial and strict procedure and rules of evidence are to be followed for doing substantial justice.

Regulatory decision making procedure involves conciliatory and facilitatory approach in most cases reaching finality at the decision by mutual consent and understanding at the quickest possible way.

Alternative regulatory dispute resolution practice is preferred to long drawn adversarial adjudicatory system consisting of stages of trial, appeal and revision.

Except few constraints as to budget, manpower and creation of posts etc. BTRC enjoys unfettered power and authority in decision making.

There is no appellate authority against the decision of the BTRC.

K. Decisions of BTRC, their nature and finality:-

The decisions of the BTRC may be classified into two categories- which are administrative decisions as routine works and the other quasi-judicial decisions which are of penal nature or of the type of dispute resolution through public hearing.

Routine decisions such as granting of licenses, approval of tariff, allocation of frequency and the like are usually taken upon compliance with certain provisions of law and procedure.

Decision on complains or disputes or on penal measure such as refusal, suspension, withholding or cancellation of Licence or injunction or enforcement order or imposition of administrative fine are taken upon hearing the parties and taking evidence, the process based on the principles of natural justice.

BTRC has power to compel witnesses to appear and give evidence or produce document the powers which are available to a civil

court under the Code of Civil Procedure 1908. Non-compliance or defiance with the direction of BTRC constitutes contempt of court punishable under the Contempt of Courts Act, 1926.

BTRC has to decide as to the institution of any prosecution against the violators of telecom law or the offenders upon scrutiny of each and every case.

The important power of the BTRC is that it has the full power of investigation of the offence under this Act by its authorized officer who can exerciser all the powers of a police officer in charge of a police station including seizure and arrest.

BTRC is vested with exclusive powers of decision making both administrative and quasi-judicial against which there is no provision for appeal or revision.

BTRC in all these sense is independent with full and final power of taking decision. It is accountable to the Parliament through the Minister of MOPT.

BTRC is composed of highly experienced persons having specialized expertise in the legal, technical, administrative and commercial fields the most concerned areas of telecommunication sector. Commissioner in the legal side has to be a person duly qualified to be a judge of the High Court

Division of the Supreme Court. Every commissioner of the BTRC currently composed of has each more than 30 years experience in their respective fields.

This means the issues of legal, technical, commercial and administrative nature are expected to be best addressed and taken care of in the decision making by the BTRC in preference to the decision of the traditional court and the High Court

Division where experts from all these branches of knowledge and expertise may not be available.

In addition to its own expertise there is provision in the Act for pleading the case of a party either personally or through expert agent or an advocate. BTRC can also take the assistance of consultants where necessary.

The decision making process of the BTRC reflects the best way of alternative dispute resolution mechanism in the most important and emerging telecommunication sector where transaction of business demands quick dispensation in the interest of economy and development.

L. Scope of judicial review of the decision of the BTRC:

BTRC is a collegial commission of 5 members where there may be less chance of corruption and arbitrariness. However the scope of judicial review is there under the constitutional provision under article 102.

The High Court Division under its extra-ordinary writ jurisdiction can scrutinize the legality or propricty of any action/decision of public officials or statutory body under article 102 of the Constitution of the People's Republic of Bangladesh. The problem of delay in disposal of cases in the High Court Division is also there which has negative impact on the growth and development of economically most violable project. Delay costs much and in many cases frustrates the purpose of justice at the end of the day.

M. Licencing Service in Bangladesh:-

Bangladesh adopted open licensing regime for ISP, VSAT and PSTN service.

Recently some steps have been taken to introduce open auction system as one of the mechanisms for granting license; and

VOIP and Network Service have been included in the Regulations and in the schedule for granting license.

In view of limited service spectrum resource granting of license for cellular mobile phone service is being done through competitive bidding procedure. Number of licenses so far granted

Mobile communications and the Internet were the two major demand drivers for telecommunication services in the last decade of the twentieth century. Combine the two; mobile Internet has one of the major demand drivers of the first decade to the twenty first century.

The convergence to mobile communications and the Internet should produce innovations 3G Internet, new applications and new services that would not otherwise be possible. The service of knowing the location of a particular mobile user, combined with the service of targeted advertising, should theoretically make it possible for local businesses to attract users that are passing by, within a certain radius. Similarly, Multimedia Messaging Services (MMS) should open up visual, more exciting person-to-person communications.

Previous experience of technological innovations such as digital networks or even cellular radio itself, has shown that

commercial fruit of the mobile internet may be some ten or fifteen years away. The cellular radio based mobile phone itself took over 20 years from the first demonstration longer to breakthrough.

With governments throughout the country Bangladesh is committed to increase access to telecommunications services and the resulting economic and social benefits; it seems highly likely that Bangladesh becomes the Region's biggest telecom market, Next to India.

Distance education and telemedicine are the two ways in which developing countries like Bangladesh can use ICT to overcome these shortages. For these two services to be effective, they require a broadband platform. Further, while demand for individual broadband access may be perceived to be low, demand for shared public access places such as internet cafes is high. Industry analysts are optimistic about the sustained growth in broadband access such as hubs and routers, cable and DSL modems. The market is also being fuelled by an exceptionally high degree of innovation like the 3 G/ GPRS systems. New services are being offered all the time. Such as metro Ethernet internet access and managed wireless LAN services.

Telecommunications may be in the doldrums in the rest of the world, but there is still something of a boom going on in Asia. In 2001 China became the world's biggest mobile market surpassing the United States. In 2002, China's biggest operator, China Mobile, became the world's largest carrier in subscriber terms. Like this in Bangladesh, we also see that our Mobile operators are also dominating the telecom market by emerging as a huge level of subscribers.

The region's general development is racing ahead by global standards, despite painful economic setbacks of recent years. Asia has, admittedly in pockets, long been a pioneer in mobile. Tokyo was home to one of the world's first cellular radio system back in 1979. Japan has been a pioneer of personal communications (creating the world's first super small handsets and microcellular infrastructures to support them) and non-voice mobile communications (with the i-mode mobile internet service). The Republic of Korea has been the leader in implementing CDMA as a basis for 3G.

An Un-official English Text of

THE BANGLADESH TELECOMMUNICATION ACT, 2001

(Act No. 18 of 2001)

CHAPTER I

PRELIMINARY MATTERS

An Act to provide for the establishment of an independent Commission for the purpose of development and efficient regulation of telecommunication system and telecommunication services in Bangladesh and matters ancillary thereto ;

Whereas it is expedient to provide for the establishment of an independent Commission for the purpose of development and efficient regulation of telecommunication system and telecommunication services in Bangladesh and for the transfer of the powers and functions of the Ministry of Post and telecommunication to the Commission and matters ancillary thereto; Now, therefore, it is hereby enacted as follows:-

1. Short title and commencement.- (1) This Act may be cited as the Bangladesh Telecommunication Act, 2001.

(2) It shall come into force on such date as the Government may, by notification in the official Gazette, specify.

2. Definitions.- In this Act, except where the subject or context otherwise requires-

"broadcasting" means transmission of any message, information, signal, sound, image or intellectual expression by radio wave, satellite, cable or optical fibre connection for the purpose of receipt by the public, but transmission of anything by Internet connection shall not be deemed to be a broadcasting *{ref. clause(30)};*

[**N.B.- The definitions are arranged in English alphabetical order and the reference to the relevant clause of this section is mentioned at the end of each definition within brackets.] -

"Chairman" means the Chairman of the Commission *{ref. clause (9)};*

"charge" means a charge to be paid for the service provided by the Commission or an operator *{ref. clause (10)};*

"**Commission**" means the Bangladesh Telecommunication Regulatory Commission established under section 6 *{ref. clause (3)}*;

"**Commissioner**" means the Chairman or any other Commissioner of the Commission *{ref. clause (4)}*;

"**consumer**" means a person who takes telecommunication service from an operator *{ref. clause (8)}*;

"**Criminal Procedure Code**" means the Code of Criminal Procedure, 1898 (Act V of 1898) *{ref. clause (23)}*;

"**employee**" includes an officer *{ref. clause (5)}*;

"**harmful interference**" means an adverse effect of electro-magnetic energy created from an emission, radiation or induction that-

(a) endangers the use or workability of radio communication system; or

(b) significantly reduces or obstructs the use or workability of radio apparatus, or interrupts such use or workability *{ref. clause (6)}*;

"**interference causing apparatus**" means an apparatus or device, other than radio apparatus, that interferes or is of capable of causing interference in radio communication *{ref. clause (17)}*;

"**Inspector**" means a person appointed as an Inspector under section 60 *{ref. clause (18)}*;

"**interconnection**" means the visible or invisible or logical linking of more than one telecommunication network in order to enable the users of one network to communicate among themselves or to communicate with the users of another network or to avail themselves of the service of the other network *{ref. clause(2)}*;

"**interested party**" means a person who is interested in the development of telecommunication or who has applied for a licence for establishing or operating telecommunication system or for providing telecommunication service, or who is interested in the activities that may be undertaken under a licence *{ref. clause (1)}*;

"**licence**" means a licence issued or deemed to have been issued by the Commission under this Act for establishing or operating a telecommunication system or for providing telecommunication service or for operating or maintaining such system or service or for using a radio apparatus *{ref. clause (29)}*;

"**Minister**" means the Minister in charge of the Ministry or Division dealing with post and telecommunication *{ref. clause (27)}*;

"**Ministry**" means the Ministry or Division dealing with post and telecommunication *{ref. clause (28)}*;

"**operator**" means a person licenced for establishing or operating a telecommunication system or providing telecommunication service or operating a system which is the combination of more than one of those facilities *{ref. clause (19)}*;

"**permit**" means a permit issued or deemed to have been issued under section 40(2) or CHAPTER-XIII *{ref. clause (21)}*;

"**person**" includes an individual having natural personality, a partnership, society, company, corporation, co-operative society and statutory body *{ref. clause (24)}*;

"**radio apparatus**" means a device or combination of more than one device suitable for use in radio communication *{ref. clause (25)}*;

"**radio communication or radio**" means emission, transmission or reception of any sign, signal, picture, image, symbol or sound by means of radio wave of a frequency lower than 3000 Ghz and propagated in the space without any artificial guide *{ref. clause (26)}*;

"**regulation**" means regulations made under this Act *{ref. clause (20)}*;

"**Spectrum Management Committee**" means the Spectrum Management Committee constituted under section 56 of this Act *{ref. clause (31)}*;

"**tariff**" means a tariff approved by the Commission under CHAPTER-VI of this Act or a tariff mentioned in section 92 *{ref. clause (16)}*;

"**technical acceptance certificate**" means a technical acceptance certificate issued by the Commission under section 57 *{ref. clause (7)}*;

"**telecommunication**" means transmission and reception of any speech, sound, sign, signal, writing, visual image or any other intellectual expression by way of using electricity or electro-magnetic or electro-chemical or electro-mechanical energy through cable, pipe, radio, optical fibre or other electro-magnetic or electro-chemical or electro-mechanical or satellite communication system *{ref. clause (11)}*;

"**telecommunication apparatus**" means an apparatus used for transmission or reception of anything that falls within the purview of the definition of telecommunication *{ref. clause (12)}*;

"**telecommunication network**" means a combination of a set of nodes and links that establish telecommunication between two or more points *{ref. clause (14)};*

"**telecommunication service**" means any of the following services:-

(a) transmission or reception, with the help of a telecommunication system, of anything that falls within the purview of the definition of telecommunication;

(b) any value added telecommunication service (e.g. fax, voice mail, paying service);

(c) internet service;

(d) supply of information or directory relating to a telecommunication system for the convenience of using a service intentioned in (a),

(b) and (c) above;

(e) a service for installation, or maintenance of telecommunication apparatus, or a service relating to the adjustment, alteration, repair, moving or replacement of such apparatus *{ref. clause (15)};*

"**telecommunication system**" means a combination of the telecommunication apparatus (e.g. switching system, transmission apparatus, terminal apparatus, satellite etc.) whether or not these equipments are visibly connected with one another, or whether or not they are combinedly used in the transmission or reception of any information or message *{ref. clause (13)};*

"**terminal apparatus**" means a telecommunication apparatus which is used by a consumer of telecommunication service for sending or receiving an information or message through a telecommunication system *{ref. clause (22)};*

"**universal service**" means providing telecommunication service to any citizen of Bangladesh or to other persons irrespective of their place of stay or occupation in Bangladesh *{ref. clause (32)}.*

3. Application.- (1) This Act shall extend to the whole of Bangladesh and also to the following :-

(a) any vehicle, vessel, aircraft or satellite;

(b) any platform, rig or other structure that is fixed in the sea or attached to the submarine land : Provided that if Bangladesh is a party to aninternational treaty, or an arrangement of similar nature in relation to a foreign vehicles, vessels, aircrafts or satellites, this Act shall apply subject to such treaty or arrangement.

(2) This Act shall not apply to the following:-

(a) any broadcasting;

(b) a radio broadcasting station or a television broadcasting station or licensing of such station;

(c) broadcasting apparatus or an apparatus for receiving any message or other information or a programme transmitted by way of broadcast, or the business of such apparatus; Provided that this Act shall apply to the following :

(i) allocation of frequency for such radio station or television station or broadcasting apparatus, or control of the allocated frequency;

(ii) use of a telecommunication apparatus in combination with broadcasting apparatus or use of telecommunication apparatus for the purpose of broadcasting.

(3) The Government may, by an order notified in the official Gazette, exempt any person or class of persons, or any particular telecommunication apparatus or radio apparatus or any particular service from the operation of any or all the provisions of this Act or of the regulations made thereunder.

4. Application of other laws etc. relating to telecommunication.- (1) The Telegraph Act, 1885 (XIII of 1885) and The Wireless Telegraphy Act, 1933 (XVII of 1933) shall, subject to the provisions of this Act, apply and where, in relation to any matter, this Act conflicts with any of those two Acts, the provisions of this Act shall prevail.

(2) For the purposes of performing the functions under this Act, the provisions of the rules or regulations made or other similar instruments, order, instructions or directions issued, under the aforesaid two Acts shall apply, so far as they are consistent with the provisions of this Act, until such rules, regulations, other similar instruments, order, instruction or directions are repealed by the Commission.

5. Act to override other laws.- Notwithstanding any contrary provisions of any other law, the provisions of this Act shall have effect.

CHAPTER II

ESTABLISHMENT AND CONSTITUTION OF COMMISSION

6. Establishment etc. of Commission.- On the commencement of this Act, a Commission to be known as the Bangladesh Telecommunication Regulatory Commission shall be established.

(2) The Commission shall be a body corporate having perpetual succession and a common seal, and shall have rights to acquire and hold movable and immovable property, to transfer such property, to enter into contract, to undertake any other activity and to take any action under this Act; and it can sue and be sued in its own name.

(3) The common seal of the Commission shall be of such size and shall contain such particulars as the Commission may determine; it shall be kept in the custody of the Chairman and shall be used in such cases as the Commission may determine :

Provided that the common seal shall not be used on any document unless the Chairman and another Commissioner are present; and they shall, to mark their presence, sign the document on which the seal is so used.

7. Constitution of Commission.- (1) The Commission shall consist of 5 (five) Commissioners, and the Government shall appoint one of them to be the Chairman and another to be the Vice-Chairman.

(2) At least two of the Commissioners shall be engineers as specified in clause–

(a) of sub-section 10(1), and at least one shall be a person as specified in clause

(b) of that sub-section, and another shall be a person as specified in clause (c) of that sub-section.

(3) No act or proceedings of the Commission shall be illegal nor shall it be called in question in any court only on the ground of a vacancy in the office of a Commissioner or a defect in the constitution of the Commission.

8. Office of Commission.- The principal office of the Commission shall be situated in Dhaka, however the Commission may, with prior approval of the Government, establish branch office at any place of the country.

9. Appointment and tenure of Commissioners.- (1) The Commissioners shall be appointed by the Government and they shall perform their functions on full-time basis.

(2) A Commissioner shall, subject to the provisions of this Act, remain in office for a period of three years from the date of his appointment and he may be reappointed for only one more tenure of that duration: Provided that no person shall be eligible for appointment to, or holding the office of, Commissioner if he attains the age of 65 (sixty five) years.

10. Qualifications and disqualifications of Commissioners.- (1) A Commissioner shall be a person who-

(a) is an engineer having at least 15 years' practical experience in the field of telecommunication;

(b) is an advocate or a judge having 15 years' practical experience in law including the qualification for appointment of a judge of the High Court Division;

(c) has 15 (fifteen) years' practical experience in business or industry or finance or economics or protection of consumer interest or management or administration.

(2) No person shall be qualified for appointment to, or for holding, the office of Commissioner, who-

(a) is not a citizen of Bangladesh;

(b) has been elected a member of the Parliament or of any local government or has been nominated as a candidate for such election;

(c) has been declared or identified by the Bangladesh Bank or by a bank or financial institution or by the court as a defaulter loanee of that bank or institution;

(d) has been declared by the court as a bankrupt and has not been discharged from that liability;

(e) has been, on conviction for a criminal offence involving moral turpitude, sentenced to imprisonment for a term of two years or more, and a period of five years has not elapsed his since release from such imprisonment;

(f) is, after being appointed Commissioner, directly engaged in any income generating activity outside the responsibilities of his office;

(g) is, in the capacity of an owner, shareholder, director, officer, partner or consultant, directly or indirectly interested in the following :-

(i) a firm or company or other organization which requires a licence or technical acceptance certificate or permit under this Act for establishing or operating a telecommunication system or for providing telecommunication service : Provided that a member or officer of the board of directors, by whatever name called, of a statutory body may be appointed as a Commissioner if he discontinues his service in that body; or

(ii) any farm or company or corporation or other organization which is a telecommunication operator in a foreign country, or which manufactures or distributes telecommunication apparatus or radio apparatus in a foreign country, or which carries on business or provides telecommunication services in Bangladesh;

(h) is unable to perform the functions of his office due to physical or mental incapacity; or

(i) fails to comply with the provisions of sub-section (3) in time.

(3) If, by virtue of a will, gift or inheritance or otherwise, the interests prohibited by sub-section (2)(g) is vested in, or acquired or held by, a Commissioner-

(a) he shall, within 3 (three) months of his appointment as Commissioner or of his knowledge about such interest, inform by issuing a written notice to all other Commissioners of the fact of holding or acquiring such interest and the nature and value thereof; and

(b) the Chairman shall, with 15 (fifteen) days, issue a notice calling a meeting of the Commissioners, but where the Chairman himself has given such notice, the Vice- Chairman shall call this meeting; and where both the Chairman and Vice-Chairman have given such notice, any other Commissioner may call this meeting; and

(c) the Commission may, after consideration of the nature and value of the interest, direct the Commissioner to dispose of the interest and he shall be bound to dispose it of accordingly; and

(d) the Commission shall immediately send a copy of such direction to the Ministry : Provided that the Commissioner acquiring or holding such interest shall not have right to vote

on the matter, although he shall be allowed to remain present in the meeting so that he may explain his position.

11. Duty of Commissioner regarding certain interest of family-members.- (1) If a member of any Commissioner's family acquires or holds any interest specified in section 10(2)(g), he shall, within three months of his appointment as Commissioner or of his knowledge about such interest, inform the Commission in writhing of the nature and value thereof.

Explanation:- In this sub-section "family" means the father, mother, husband or wife, son, daughter, step-son and step-daughter of the Commissioner.

(2) If a member of a Commissioner's family acquires or holds such interest in a firm, company, corporation or other organization, the Commissioner shall not have a right to vote in the meeting where the Commission takes any decision in respect of that firm, company, corporation or other organization, although the Commissioner may remain present in the meeting.

12. Resignation and removal of Commissioners.- (1) Any Commissioner may resign from his office by sending to the Government a written notice of three months, and a copy thereof to the Chairman or, where the Chairman himself resigns, to the Vice-Chairman : Provided that despite such resignation the Government may, pending formal acceptance thereof, request the resigning Commissioner to continue to perform his functions.

(2) A Commissioner may be removed from office, if -

(a) any situation specified in clauses (a) to (g) of sub-section 10(2) occurs; or

(b) he is found guilty of corruption, misuse of power, gross misconduct or gross negligence in duty.

(3) If the Government is of opinion that a Commissioner is unfit to hold that office on any ground specified in sub-section (2), the Government shall constitute an Enquiry Committee consisting of one or more judges of the Supreme Court, and shall also specify in the order by which the committee is constituted the time limit for submission of the enquiry report.

(4) The Committee constituted under sub-section (3) shall, on the basis of specific information and reasons, submit a report as to whether

or not the allegations brought against the Commissioner have been proved and whether or not he should be removed from his office, and the Government shall, as far as possible, take action in accordance with the recommendation contained in the report.

(5) The Government shall not remove any Commissioner under this section without giving him an opportunity of showing cause against the proposed removal.

(6) Where the Enquiry Committee is constituted under sub-section (3), the Government may, in consideration of the relevant circumstances, direct the Commissioner to refrain from performing the functions of his office, and the Commissioner shall be bound to comply with such direction.

(7) The Enquiry Committee shall be deemed to be a Commission appointed under the Commission of Enquiry Act, 1956 (VI of 1956) and the provisions of that Act shall, subject to this Act, apply to the Committee.

13. Filling in casual vacancy in Commissioner's office.- Where the office of a Commissioner falls vacant due to his death, resignation or removal, the Government shall, within 30 days of such vacancy, appoint a competent person to the vacant office.

14. Chief executive.- The Chairman shall be the chief executive of the Commission; and where the Chairman is unable to perform the functions of his office due to resignation, removal, absence, illness or any other cause, the Vice-Chairman shall be competent to exercise all the powers and perform all the functions and duties of the Chairman till a new Chairman is appointed or, as the case may be, the existing Chairman is able to resume his office; and where both the Chairman and Vice-Chairman are unable to perform their functions and duties, the Government may direct a Commissioner to temporarily act as the Chairman.

15. Meetings of Commission.- (1) The Commission may, subject to the provisions of this Act, adopt general or specific resolutions in respect of the place, time and procedure of its meetings and all the meetings of the Commission shall be held in accordance with such resolutions : Provided that until such resolutions are adopted or if no resolution has been adopted on a specific matter, the meetings of the Commission shall be held in accordance with the decision of the Chairman.

(2) The presence of three Commissioners including the Chairman or, as the case may be, the Vice-Chairman, shall constitute quorum for a meeting of the Commission.

(4) The Chairman and in his absence the Vice-Chairman shall preside over all meetings of the Commission.

(5) A decision of the Commission shall be taken in accordance with the majority votes of the Commissioners present in the meeting, and in case of equality of votes, the person presiding shall have a second or casting vote.

(6) Any two Commissioners may, in writing, request the Chairman to call a meeting of the Commissioners for the purpose of holding discussion or taking decision on a specific issue, and within 7 (seven) days of receipt of such request the Chairman shall call a meeting.

(7) The Chairman may, for the purpose of presenting opinion, deliberation, information or explanation on any issue, invite any relevant person and, subject to the decision of the meeting, the opinion, deliberation, information or explanation of the person so invited may be recorded in the proceedings of the meeting.

16. Committee.- The Commission may, for the purpose of assisting it in the performance of its functions, appoint necessary committees consisting of one or more Commissioners, or any officer or employee of the Commission or any other person.

17. Status, remuneration and privileges of Commissioners.- (1) The Government shall fix the status, remunerations, allowances, privileges and other conditions of service of the Chairman, Vice-Chairman and other Commissioners.

(2) After appointment of a person as Commissioner, his status, remuneration, privileges and other conditions of service shall not be so changed that the change is unfavorable to him.

18. Appointment of Secretary, officer-employees etc. of Commission.- (1) The Government shall appoint the Secretary to the Commission.

(2) The duties of the Secretary shall be to fix the agenda in accordance with the direction of the Chairman and to fix, subject to any resolution taken by the Commission in this regard, the date and time of the meetings of the Commission, to prepare the minutes of such meetings, to preserve the records and other particulars of the actions

taken by the Commission and to perform such other functions and duties as the Commission may assign to him.

(3) The Commission may, for efficient performance of its functions, appoint necessary officers and other employees and consultants, and to that end, it may take all necessary actions including the following:-

(a) with the prior approval of the Government, fixation of the number of employees to be appointed by the Commission and their salaries, allowances and other facilities;

(b) on the basis of the approved manpower, determination of the organizational structure of the Commission and division thereof into necessary working units, specifying the functions of such units, and appointment of employees to posts for which they are competent and effecting their transfer;

(c) fixation of the fees of consultants with prior approval of the Government and in accordance with applicable Government-rules, and payment of such fees;

(d) taking disciplinary actions against employees including their dismissal from service, and fixation of other conditions of their service;

(e) establishing provident fund and undertaking other schemes for the welfare of the employees and exercising control over, and making contribution to, such fund or scheme.

(4) The appointment and conditions of service of the employees shall be determined by regulations and until such regulations are made the Commission may, by administrative order, determine those matters.

19. Appointment of personnel on deputation from other organizations.- (1) The Commission may, with the consent of the respective controlling authority, appoint on deputation any employee of the Government or a statutory body, and such appointment shall be made in accordance with applicable laws and as agreed between the Commission and the said authority.

(2) A person appointed under sub-section (1) shall, while serving in the Commission, be subject to the same discipline and control as the other employees of the Commission are subjected to.

20. Employment outside Commission.- (1) A Commissioner shall not, without written approval of the Government, and a full-time

officer or employee of the Commission shall not, without written approval of the Commission, engage himself in any work for any kind of remuneration or in any work outside the Commission, nor shall he continue to be engaged in such work.

(2) Any Commissioner, or any officer or other employee of the Commission, shall not engage himself, nor shall he continue to be engaged, in any work which, in the opinion of the Government or the Commission respectively, may adversely affect the proper discharge of his functions and duties.

CHAPTER III
FINANCIAL MATTERS OF COMMISSION

21. Bangladesh Telecommunication Regulatory Commission Fund.- (1) The Commission shall have a fund to be known as the Bangladesh Telecommunication Regulatory Commission Fund, and grants from the Government, a statutory body or other local or foreign organization, loans raised by the Commission, fees and charges paid under this Act and moneys received from other sources shall be credited to the Fund.

(2) All moneys of the Fund shall be deposited with a scheduled bank as specified by the Commission and the procedure for withdrawal of money from that bank shall be determined by the Commission.

Explanation:- "Scheduled bank" means a scheduled bank as defined in section 2(j) of the Bangladesh Bank Order, 1972 (P. O. No 127 of 1972).

(3) The Fund shall be utilized to meet the expenses relating to the salaries and allowances of the Commissioners and employees and other necessary expenses of the Commission.

(4) If any money remains surplus after meeting all the expenses of the Commission, it shall be credited to the Consolidated Fund of the Republic.

22. Annual budget statement.- Every year, the Commission shall, for the next financial year, submit to the Government a budget statement within the time specified by the Government, and in such statement the estimated amount required from the Government for that financial year shall be specified; and before commencement of that financial year, the Government shall, on the basis of that statement, approve the budget of the Commission with or without modification of the statement.

23. Power to raise loan.- The Commission shall have authority to raise loan for the purpose of performing its functions under this Act and also to repay such loan; however approval of the Government shall be necessary in case of taking a foreign loan.

24. Charge etc. for services provided by Commission.- (1) The Commission may impose and realize charges or fees or both for the services provided or to be provided by it in connection with the exercise of its powers and performing its functions under this Act.

(2) The generality of the authority under sub-section (1) includes the following:-

(a) framing of one or more schemes for the purpose of specifying charges or fees for any particular service or all the services provided or to be provided by the Commission;

(b) fixation of the rates of, or determination of the accounts procedure for, such charges and fees by making regulations or, in the absence of regulations by issuing executive orders.

(3) Any charge, fee, administrative fine and dues receivable by the Commission may be realized as public demand.

25. Exemption from tax.- Notwithstanding any contrary provision of any other law, the Commission shall not be liable to pay any income tax on any property held or received or any income earned by it and the Commission is hereby exempted from the payment of such tax.

26. Realisation of dues.- (1) All charges, fees, administrative fines and other dues receivable by the Commission may be realized by it as a public demand under the Public Demands Recovery Act, 1913 (Ben. Act III of 1913).

(2) For the purposes of sub-section (1), the Commission may appoint any of its officers as a Certificate Officer as defined in sub-section 3(3) of that Act and that officer shall be competent to exercise the powers and perform the functions of a Certificate Officer under that Act.

27. Accounts and Audit.- (1) The Commission shall maintain accounts of all moneys received and spent by it; and subject to any general direction given by the Government, the Commission may determine the procedure for maintaining such accounts; however such account must accurately and properly reflect the financial position of the Commission.

(2) Within 60 (sixty) days of the expiry of every financial year, the Commission shall prepare the Accounts Statement and Financial Statement and shall, after getting them audited by a chartered accountant firm registered under the Bangladesh Chartered Accountants Order, 1973 (P.O. No 2 of 1973), make arrangements for sending such statements to the Ministry for the purpose of their presentation before the Parliament, and the Ministry shall, as soon as possible, cause the Statements along with the report specified in section 28 to be presented before the Parliament.

(3) Apart from the audit specified in sub-section (2), the Commission, as a statutory public authority within the meaning of the Comptroller and Auditor General (Additional Functions) Act, 1974 (XXIV of 1974), shall be under the jurisdiction of the Comptroller and Auditor General.

28. Report.- The Commission shall, within 90 (ninety) days of the expiry of every financial year, send to the Minister a report on the functions of the Commission during that year, and the Minister shall, as soon as possible, make arrangements for presentation of the report before the Parliament.

CHAPTER IV
BROAD OBIECTVES, POWERS AND FUNCTIONS

29. Broad objectives of Commission.- The broad objectives of the Commission are as follows:-

(a) to encourage the orderly development of a telecommunication system that enhances and strengthens the social and economic welfare of Bangladesh;

(b) to ensure, in keeping with the prevalent social and economic realities of Bangladesh, access to reliable, reasonably priced and modern telecommunication services and internet-services for the greatest number of people, as far as practicable;

(c) to ensure the efficiency of the national telecommunication system and its capability to compete in both the national and international spheres;

(d) to prevent and abolish discrimination in providing telecommunication services, to progressively effect reliance on competitive and market oriented system, and in keeping with these objectives, to ensure effective control of the Commission;

(e) to encourage the introduction of new services and to create a favourable atmosphere for the local and foreign investors who intend to invest in the telecommunication sector in Bangladesh.

30. Functions and duties of Commission.- (1) The functions and duties of the Commission shall be as follows:-

(a) to regulate the establishment, operation and maintenance of telecommunication services in Bangladesh;

(b) to protect the interests of the local consumers in respect of the charges imposed on them, and their access to telecommunication services, and the quality and variety of such services;

(c) to encourage research and development activities in telecommunication, and innovative activities and investment in providing telecommunication services;

(d) to protect the social and economic interests of the consumers, to respond to their needs, and to control and abolish the existing and probable oppressive or discriminatory conduct or activities of the telecommunication service providers;

(e) to maintain and promote competition among the service providers in order to ensure high-quality telecommunication services;

(f) to ensure protection of the privacy of telecommunication;

(g) to collect, from within and outside Bangladesh, information on telecommunication and internet and to analyse and assess their impact on Bangladesh and to take necessary action or, as the case may be, to make necessary recommendations to the Government;

(h) to frame a national scheme of numbering plan to be followed in telecommunication and to modify it whenever necessary.

(2) The generality of the functions and duties under sub-section (1) includes the following specific functions and duties :-

(a) to frame a code of practice to be followed by the local operators and another code of practice to be followed by them in their relationship with foreign operators;

(b) to inform the Minister of the licences, permits and technical acceptance certificates issued under this Act ;

(c) to adopt policies with regard to subsidy given by the same operator from the earning of one service to another service provided by him, and to take legal actions ;

(d) to carry out the responsibilities assigned and the directions issued by the Government under suction 34;

(e) to discharge the international responsibilities of the Government in the field of telecommunication in accordance with the direction of the Government or to ensure the discharge of such responsibilities through operators ;

(f) to assist the concerned Ministries in matters of the International Telecommunication Union and other international and regional organizations relating to the standards and procedure to be followed in telecommunication ; to collect the notices of the International Telecommunication Union and information on all relevant matters and to inform the relevant organizations of Bangladesh of those matters ;

(g) unless the Government otherwise directs, to represent the Government in international conferences on telecommunication matters and in meetings with foreign organizations ;

(h) to collect information relating to international and regional conferences on telecommunication and to deliver such information to the concerned Ministries or organizations; and to advise those Ministries and organizations including broadcasting organizations in sending competent delegates for participating in those conferences; and to play proper role with regard to selection of delegates and their duties ;

(i) to advise the Government or regional organizations in arranging conferences on international, regional and sub-regional basis as considered necessary;

(j) to set the technical standards and criteria of telecommunication services, to monitor the standards of telecommunication services provided by operators and to ensure that such services conform to the standards set by the commission;

(k) to make arrangements for monitoring the standards set by the Commission and their compliance;

(l) to ensure the compliance of the provisions of this Act keeping in view of public interest in general, and to protect the interest of the consumers from the unfair practices of the operators and other persons engaged in providing telecommunication services in particular;

(m) to improve the competition scenario including the discharge of the following responsibilities:-

(i) to protect an operator of a telecommunication system or a service provider from such activities of another operator or provider as are damaging to competition;

(ii) to facilitate the access of a person intending to participate as an operator in the market of telecommunication system or service;

(n) to ensure that necessary decisions on all matters are taken quickly, openly, fairly and transparently;

(o) to perform such other functions as the Government may from time to time assign, provided they are consistent with the functions and duties of the Commission and necessary finance and other resources are available;

(p) to introduce a mechanism for the purpose of receiving the objection and suggestion of consumers at regular intervals and to ensure proper action on these objections and suggestions;

(q) to arrange publicity of, and public hearings on, matters of public interest.

31 Powers of Commission.- (1) The Commission may, subject to the provisions of this Act and regulations, exercise all powers that are necessary to perform its functions and duties under section 30.

(2) The generality of the powers under sub-section (1) includes the following specific powers:-

(a) subject to payment of fees specified by the Commission in proper cases Page

(i) to issue licence for establishing or operating telecommunication system, or providing telecommunication services or using of radio apparatus, and in proper cases to issue permits and technical acceptance certificates;

(ii) to allocate radio frequency and to authorize the use thereof, to monitor the use of radio frequency and spectrum management;

(iii) to renew, suspend and cancel the licences, permits and certificates issued; to control their transfer;

(b) to hold enquiry and to take decision and necessary action on accusations and other demands raised against holders of licence, permit and technical acceptance certificate for

violation of the conditions contained therein and the provisions of this Act and regulations;

(c) to specify the procedure to be followed and other steps to be taken by operators in respect of maintaining their accounts ;

(d) to approve, keeping in view of the general policy of the Government, the various telecommunication services for which licences are necessary ;

(e) to determine, in respect of telecommunication services, the tariff, call charges and other charges and to specify the procedure for fixation thereof by the operators;

(f) to wholly or partly suspend or disallow the tariff, contract or arrangement, submitted to the Commission under this Act, if the Commission considers it to be inconsistent with this Act; and to give necessary directions;

(g) to issue guidelines on matters not sufficiently provided in this Act or regulations and, in appropriate cases, to give decisions as the Commission may deem proper and to issue orders accordingly;

(h) to issue guidelines on matters of interconnection among operators, to determine, in appropriate cases, the conditions applicable thereto, and to resolve disputes among them ;

(i) to direct the operators to submit report along with necessary information on any of their activities;

(j) to get the operator's procedure and systems audited so as to be satisfied about the compliance of the directions issued by the Commission, and to examine the propriety of the reporting system of the operators, and to g.ve directions on these matters; (k) to give necessary directions to the operators to ensure that the Commission gets sufficient opportunity to inspect the books and records of the operators and to monitor their activities;

(l) to direct an operator to submit to the Commission his annual plan of capital expenditure so that the Commission can analyse and assess and thus gets sufficient idea about the monopoly business, if any, of that operator in providing telecommunication services in a particular area;

(m) to appoint consultants to assist the Commission in exercising its powers, in performing its functions and duties under this Act and matters relating thereto;

(n) to issue enforcement orders to ensure compliance with the provisions of this Act and, in appropriate cases, to impose and realize administrative fines;

(o) to approve each site on which radio apparatus including antenna system may be installed and to approve erection of each mast, tower, support-structure and construction of other related structure;

(p) to direct an applicant for or a holder of a licence to furnish any information which the Commission considers necessary with regard to the proposed or existing use of a radio apparatus, its installation and maintenance, and also any major change in the apparatus;

(q) to take any other action that is necessary for the development of telecommunication and its orderly and efficient operation;

(r) to issue and publish instructions to be followed in relation to activities of the Commission under this Act, instructions to be followed by licensees and service providers and also instructions on matters relating to terminal apparatus, telecommunication apparatus, interference causing apparatus, radio frequency and radio apparatus;

(s) to specify, by making regulations, the modes of exercising powers and related matters on which powers are given by this sub-section but no specific provision is made in this Act.

32. Delegation of power by Commission.- The Commission may, by regulation or by general or special order, whether absolutely or conditionally, delegate any of its powers, but not the powers under this section and section 99, to the Chairman or any other Commissioner, or to any of its officers or employees or other person.

33. Functions of the Ministry.- (1) The functions of the Ministry shall be to determine the general policy of the Government in the telecommunication sector and to encourage the development of that sector in Bangladesh.

(2) The generality of the functions under sub-section (1) includes the following specific functions and duties :-

(a) to take appropriate actions to facilitate exchange of information on telecommunication within and outside Bangladesh;

(b) to identify the area where telecommunication technology can be applied for the purpose of developing and flourishing the local culture and social bondage; and to encourage the use of such technology in those areas;

(c) to identify the fields of public and private sector investment for the purpose of developing an effective and modern telecommunication infrastructure and to encourage such investment on the basis of cooperation between the public and private sectors;

(d) to undertake, on its own, research and development initiatives in telecommunication in Bangladesh and also to undertake such initiatives jointly with regional and other organizations interested in this regard;

(e) to undertake educational and training programs for human resources development of enterprises which establish telecommunication system, provide telecommunication services and manufacture related products;

(f) to assist, where possible, the Commission and other organizations for the purpose of enhancing the local telecommunication manufacturing capability and developing the innovative telecommunication services;

(g) to assist the Commission, on its request, to control or abolish discrimination or discriminatory conduct in providing telecommunication services or in extension of such services;

(h) to arrange a forum where the Ministry, Government, Commission, operators, consumers and other interested persons may meet to discuss matters of common interest;

(i) to co-ordinate participation of Bangladesh in the activities of the International Telecommunication Union and other international organizations regarding policies, standards and procedure to be followed in telecommunication and training on such matters;

(j) to dispose of all applications and other correspondence made to it under this Act, and to expeditiously execute its decisions.

34. Powers of Government.- The Government may, under this Act-

(a) take all necessary actions in order to establish its rights and discharge its obligations under international laws and

regulations or any international agreement relating to telecommunication;

(b) from time to time, refer to the Commission any matter relating to telecommunication for its consideration and recommendations thereon;

(c) consult the Commission on any matter that the Government considers proper;

(d) undertake research on telecommunication, radio communication and such technical matters of broadcasting as are related to the said communications, or may finance or otherwise assist those research activities;

(e) direct the Commission to represent Bangladesh in meetings of international and regional telecommunication organizations.

CHAPTER V

Licences for telecommunication etc.

35. Requirement for licence for telecommunication, internet etc.- (1) Subject to sub-section (3), no person shall, without a licence-

(a) establish or operate a telecommunication system in Bangladesh or undertake any construction work of such system;

(b) provide in Bangladesh or to any place outside Bangladesh any telecommunication service;

(c) undertake any construction work for providing internet service or install or operate any apparatus for such service.

(2) A person commits an offence if he contravenes sub-section (1), and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 10 (ten) years, or to a fine not exceeding 10 (ten) lac taka or to both.

(3) No licence shall be required for the following:-

(a) to operate a telecommunication system which is not connected to another telecommunication system and all its apparatus are-

(i) situated in the same premises and meant only for the use of the owner, tenant or occupant of that premises; or

(ii) installed in only one vehicle, vessel or aircraft, or installed in more than one vehicle, vessel or aircraft which are mechanically connected with one another;

(b) a telecommunication system which is operated by a single person or by a single organization , and which is not connected in any way to another telecommunication system, and

(i) that person or organization alone controls all the apparatus of that system;

(ii) all the message and information transmitted by that system are used only by the that person or organization; and

(iii) no radio apparatus is used in that system;

(c) installation of a terminal apparatus in the telecommunication network of an operator;

(d) establishment of a telecommunication system or providing telecommunication service by the Police, Bangladesh Rifles, Coast Guard, any of the defences forces or any other security force specified by the Government for its own requirement ;

(e) telecommunication system established, used, or telecommunication services provided, by the Ministry of Foreign Affairs or any intelligence agency of the Government for its own requirement ;

(f) telecommunication system established in, or used by, a battle-ship or defence-aircraft engaged in state affairs.

36. Exclusive authority of Commission to issue licence and its procedure.- (1) The Commission shall have exclusive authority to issue licence for activities specified in clauses (a) to c) of section 35(1), and to obtain such a licence, an application is to be submitted to the Commission.

(2) The Commission may, in accordance with the provisions of this Act, allow or disallow an application submitted to it under sub-section (1); while considering such application, the Commission shall, among others, consider the following aspects:-

(a) whether the applicant is disqualified under sub-section (3);

(b) whether he has sufficient financial capacity to operate the activities for which the application has been submitted, and whether he is likely to acquire the space for necessary installations and whether efficient manpower will be available;

(c) how far the issuance of the licensee applied for will be consistent with the broad objectives of the Commission specified in section 29;

(d) whether issuance of the licence applied for, the activities authorized by the licence and the terms and conditions of the licence, will be discriminatory compared to those of the existing licence holders, and whether the competition scenario will be affected;

(e) how far the issuance of the licence applied for will serve the public interest.

(3) A person shall be disqualified for obtaining a licence, if-

(a) in the case of an individual-

(i) he is an insane person;

(ii) he has been sentenced by a court under any law, other than this Act, to imprisonment for a term of 2 (two) years or more, and a period of 5 (five) years has not elapsed since his release from such imprisonment;

(iii) he has been sentenced by a court for commission of any offence under this Act and a period of 5 (five) years has not elapsed since his release from such imprisonment;

(iv) he has been declared bankrupt by the court and has not been discharged from the liability of bankruptcy;

(v) he has been identified or declared by the Bangladesh Bank or by the court or by a bank or financial institution as a defaulter loanee of that bank or institution; or

(vi) his licence has been cancelled by the Commission at any time during the last 5 (five) years;

(b) the applicant being a company or corporation or partnership or society or other organization,-

(i) any provision of sub-clauses (i) to (v) of clause (a) is applicable to its owner or to any of its directors or partners; or

(ii) sub-clause (vi) of that clause is applicable to it.

(4) Where under this section

(a) a person applies for issuance or renewal of a licence, he shall pay the fees determined by the Commission;

(b) a licence is issued, the validity period thereof, the requirement for its renewal and the conditions applicable thereto, shall be mentioned in the licence;

(c) a licence is issued for providing service, the service to be provided by the operator shall be specifically mentioned in the licence ;

(d) a licence is issued for the establishment of a telecommunication system and for providing a service, the service shall be provided through that system as mentioned in the licence;

(e) a licence is issued and the use of radio apparatus, interference causing apparatus and radio frequency are necessary to carry on the activities there under, a condition shall be mentioned in the licence that, under CHAPTER-VIII, another licence and allotment of radio frequency and technical acceptance certificate shall be obtained.

(5) Every application for licence shall be submitted to the Commission in such form and in such manner as may be specified by it.

(6) The Commission may consider the issuance of a new licence for which an application is submitted pursuant to a tender notice: Provided that the Commission may identify certain services for which licence may be issued by it without a tender notice.

(7) The Commission may, for the purpose of considering an application for licence, require the applicant to furnish necessary information and documents, and if necessary, may also inspect the location, installations and apparatus proposed by the applicant.

(8) If -

(a) such application is submitted to the Commission, it shall, within 180 (one hundred and eighty) days from submission thereof, take a decision to allow or reject it; and where it so allows, it shall inform the applicant of its decision within 7 (seven) days thereafter;

(b) The Commission decides within that period to reject the application, it shall, within 7 (seven) days of the decision, informs the applicant of such decision along with the reasons therefore;

(c) The Commission finds that it is not possible to take any decision within the said 180 (one hundred and eighty) days, it shall, within that period or within 7 (seven) days thereafter, inform the applicant of the reasons for the delay and the probable time-limit within which decision may be taken and shall take a decision within the said probable time-limit.

(9) The Commission shall preserve a printed copy of each licence issued by it and any person may, on payment of the fees specified by the Commission, inspect such copy or collect a copy thereof.

37. Conditions of licence.- (1) A licence or any right acquired there under, whether wholly or partly, shall not be transferable, and such transfer, if any, shall be void.

(2) The Commission may specify in the licence any condition consistent with this Act and regulations and, to suit the requirements of a particular situation, it may also specify additional conditions.

(3) Within the purview of the generality of sub-section (2), proper conditions with regard to all or any of the following specific matters may be included in a licence:-

(a) compliance with this Act and regulations by the licensee ;

(b) for the purpose of ensuring access to the service specified in the licence to people of the rural and sparsely populated areas, compulsory obligation of the licensee to provide the service but not exceeding 10% of his capacity ;

(c) payment of the fees or other dues specified by the Commission to meet the expenses that the Commission may incur in connection with issuance or renewal of the licence or with both ;

(d) delivery, at such time and in such manner as may be specified by the Commission, of all such documents, accounts, estimates, return or other information as the Commission may require in connection with the performance of its functions and duties under this Act and regulations;

(e) taking of the following steps by the licensee:-

(i) to design and to maintain his telecommunication network in accordance with the directions of the Commission in relation to the establishment of the telecommunication system under the licence or in relation to the transmission plan, signaling plan, switching plan and numbering plan for providing service under the licence; and in case of deviation from such plan, to obtain approval and directions of the Commission, and implementation of such direction;

(ii) inform the Commission of the routes used and the system followed in transmitting and receiving message, signal or any other information in the national and international spheres;

(f) specifying the matters relating to the telecommunication system to be used by the licensee, the services provided or to be provided by him, the coverage area of such system and services, and the period thereof;

(g) prohibition on showing any preference to, or making any discrimination against, a particular person or class of persons, in case of providing service, giving connection or permission by the licensee;

(h) ensuring an information system so that all information relating to bills, prices, directories, inquiries and complains are easily available to the consumers;

(i) where the licensee is a company, society or partnership, the compulsory obligation of such licensee to take prior approval of the Commission in the following cases:-

(i) any change in the ownership or share capital of the company, society or partnership, which has the effect of transferring the control over the activities under the licence; or

(ii) merger of the company, society or partnership with any other company or enterprise : Provided that, while giving such prior approval, the Commission shall consider whether or not the person, company or enterprise, who or which will acquire control over the licensed activities due to the proposed merger or change, is eligible for obtaining a licence, and whether or not the change will affect the continuity of those activities;

(j) publication of notification by the licensee, at such intervals and in such manner, as the Commission may specify, relating to the charges for, and the conditions applicable to the availing of, the services provided;

(k) ensuring the payment of compensation to persons affected by the under ground cable, overhead cable and accessories;

(l) making of plans showing how the licensee intends to ensure the continuity or, as the case may be, restoration of telecommunication system established or the services provided, and submission of such plan;

(m) keeping, transferring or disposing of telecommunication apparatus and other property;

(n) real performance of the standardised service, maintenance of technical standards and compliance with other technical conditions;

(o) obligations of the licensee with regard to conservation of environment in accordance with prevalent laws;

(p) other matters as the Commission may consider appropriate and expedient.

38. Renewal of licence.- A licence issued under this Chapter may be renewed in such manner and subject to payment of such fees or other payment as may be prescribed by regulations, and in the absence of regulations as may be specified in the administrative orders issued by the Commission.

39. Amendment of conditions of licence.- (1) The Commission may, for the purposes of this Act, amend any condition of any licence issued under this Act by way of alteration substitution, addition, omission or other modification.

(2) Where the Commission, on its own initiative, directs any amendment in the conditions of a licence, it shall serve a notice on the licensee informing him of the reasons for the proposed change and also directing him to submit his reply, within 15 (fifteen) days; and if any reply is submitted, the Commission shall, consider it and take its decision within a period not exceeding 30 (thirty) days thereafter.

(3) The Commission may also, upon application, amend any condition of a licence which it considers proper.

40. Restrictions on according commercial permission for use of telecommunication system.- (1) An operator shall not, without a permit issued by the Commission, accord permission to any other person or allow him, on commercial basis or in lieu of fees, price or other consideration, to use his telecommunication system or any installation or apparatus or facility by which telecommunication services can be provided.

(2) Where an operator applies for a permit mentioned in sub-section (1), the Commission may allow the application and issue a permit if, after necessary inquiry, it is satisfied that the permit applied for will not adversely affect the telecommunication system or the providing of its services, and may also impose such conditions as it considers appropriate in any particular circumstances; the permit so issued shall remain valid for a period specified therein.

(3) Where a condition mentioned in the permit issued under sub-section (2) is violated, the Commission may at any time cancel the permit.

(4) An operator commits an offence if he contravenes the provision of subsection (1), and for such offence he shall be liable to be sentenced-

(a) in the case of a first offence, to imprisonment for a term not exceeding 3 (three) years, or to a fine not exceeding 3 (three) lac taka, or to both;

(b) in the case of each subsequent offence, to imprisonment for a term not exceeding 5 (five) years or to a fine not exceeding 5 (five) lac taka or to both.

41. Commission's jurisdiction in case of limiting operator's liability.- If a licensee, for the purpose of limiting his own liability, imposes any condition in relation to a service provided by him and if the Commission considers such condition to be unreasonable, it may direct the licensee to cancel the condition and accordingly he shall be bound to comply with the direction.

42. Right of way.- (1) Subject to the other provisions of this section, an operator shall have right to install any apparatus, thing or facility on, above or over any land for the purpose of establishing a telecommunication system or for providing telecommunication service; such right is referred to in this Chapter as the right of way.

(2) Within the purview of the right of way, an employee or representative of the operator authorized in writing in this behalf may-

(a) by giving reasonable notice, enter any land at any time, and put up any post or pillar for the purpose of holding or supporting any telecommunication apparatus;

(b) fasten or attach a bracket or other device to a tree standing on the land ;

(c) cut down any tree or branch of a tree which is causing or is likely to cause injury to, or which impedes or is likely to impede the workability of, such apparatus, thing, facility or device; and

(d) take any other necessary step or action under this Act for the purpose of installing, constructing, examining, repairing, changing, removing or increasing the workability of such apparatus, thing, facility or device.

(3) An operator shall ordinarily exercise his right of way on the land owned or possessed by the Government or a local authority or statutory body, but may, if necessary, exercise this right on any other land also; the Government agency or the local authority or the statutory body shall not ordinarily obstruct the exercise of the right of way.

(4) In exercising the right under sub-section (1), the operator-

(a) shall not enter, or do anything under that sub-section in a graveyard or crematorium or a place which contains something that is regarded by the local people as sacred, unless such entry is necessary for the purpose of removal or repair of a thing which is dangerous to life or property or which impedes its security ;

(b) may, in case of necessity for such removal or repair, enter the graveyard, crematorium or sacred place with the consent of the person in charge thereof, or if there is no such person at all or if he is not readily available or if he refuses to give consent, the operator may so enter or may take steps or other actions under sub-section (1) after obtaining written permission of the Commission.

(5) The said operator-

(a) shall not, without the consent of the owner or occupier of the land, exercise his right under sub-section (1);

(b) shall not acquire any other right only because of his right of way;

(c) shall not exercise any right under this section on the land owned or controlled by any Government or local authority or a statutory body without its consent;

(d) shall exercise the rights under this section in such a manner that the damage caused to the land and environment remains at the minimum level, and shall be bound to pay compensation to the affected person, authority or body for the damage caused as a result of such exercise.

(6) The notice under sub-section (2)(a) shall contain a full and proper description of the intended work and shall be served on its receiver personally or his representative or his relevant employee, or it shall be sent to his residence or place of work.

(7) Where a telecommunication apparatus or radio apparatus becomes a cause of threat to anyone's life or property, the operator may enter a land without permission of the its owner or occupier of the land, and take necessary steps for the purpose of protecting such life and property.

(8) In exercising the powers under this section, the operator shall take all reasonable care and shall in all cases Page

(a) restore, as far as practicable, the damaged structure, service or facility, by way of repair or otherwise, to its pre-damaged condition:

(b) remove all dirt or debris from the work-site;

(c) pay compensation to the owner or occupier or person-in-charge of the damaged property.

(9) The owner or occupier or person-in-charge may, within 5 (five) days of receipt of the notice under sub-section (6), submit to the Commission a written objection, and where such objection is submitted, the Commission shall, within 15 (fifteen) days, enquire into the objection and give its decision thereon; such decision shall be binding on both the operator and the objector; and the decision shall not be called in question before any court or other authority.

43. Refusal of consent of owner etc. to the exercise of right of way.- (1) If an owner, occupier or person-in-charge does not give or refuses to give the consent or permission specified in section 42(5), or obstructs the exercise of the right of way, the operator may submit to the Commission a report on the matter.

(2) Where a report under sub-section (1) is submitted and the Commission, after such inquiry as it considers appropriate, is satisfied about the operator's necessity to enter the land, the Commission may-

(a) take such steps as it considers appropriate for obtaining the consent or permission or for the exercise of the right of way;

(b) where necessary, authorize the operator to enter the land and also request the law enforcing agencies to assist the operator so that the authorization is executed; and the law enforcing agencies shall, in order to ensure the exercise of the right of way in relation to the concerned land, take necessary steps including application of force.

(3) Where the Commission, under sub-section (2), requests a Government or local authority or a statutory body for ensuring an operator's right of entry, such authority or body shall, unless there is a special reason, comply with the request; in case of disagreement, the Commission shall immediately inform the Minister of the matter, and he shall, within a period not exceeding 15 days, consult the relevant

Minister-in Page charge and give his decision on the matter; such decision shall be final and all parties concerned shall be bound to comply with the decision, and the legality or propriety of the decision can not be called in question before any court or other authority.

44. Compensation.- (1) The operator shall pay compensation to the affected person or authority for any damage resulting from the exercise of the right of way under section 42 or anything done under section 43; such compensation shall be paid within 90 (ninety) days after completion of the work.

(2) Where a dispute arises as to the amount of compensation mentioned in sub-section (1), the affected person, authority or body shall refer the dispute to the Commission and the decision of the Commission on the matter shall be final, and the decision shall not be called in question before any court or other authority.

(3) Any claim for, or dispute over, the compensation may be submitted to the Commission within three years after completion of the work of the operator which has resulted in damage, and the Commission shall reject any claim for compensation that is raised after the expiry of that period; the legality or propriety of the decision of the Commission on the matter shall not called in question before any court or other authority.

45. Compulsory acquisition of private land for licensee's necessity.- (1) Where, in carrying out the activities under a licence, the licensee faces obstruction to use a land, or the consent of the owner or occupier of the land is not available, the Government may, on the recommendation of the Commission, decide under the Acquisition and Requisition of Immovable property Ordinance, 1982 (II of 1982) that the land is necessary for carrying out such activities of the licensee, and thereafter necessary proceedings for acquisition of the land may be initiated.

Explanation.- For the purposes of this sub-section, "land" does not include a land owned or occupied by a Government authority or a local authority or a statutory body.

(2) Where a decision in relation to a land is given under sub-section (1), the land shall be deemed to be necessary in public interest within the meaning of the Acquisition and Requisition of Immovable Property Ordinance, 1982 (II of 1982).

(3) The compensation and other costs incidental to the acquisition under this section shall be paid by the operator.

46. Cancellation and suspension of licence.- (1) The Commission may, at any time, suspend or cancel a licence, if the Commission has reasons to believe that the licensee-

(a) is at present such a person that if he were an applicant for a licence, his application would have been disallowed on any of the grounds specified in sub-section 36(3);

(b) had obtained the licence by suppressing his disqualification specified in that sub-section ;

(c) has failed to start providing the service within the time-limit specified in the licence; or

(d) has contravened any provision of this Act or regulations made there under or any condition of the licence.

(2) The Commission shall serve on the licensee a notice specifying the reasons for the proposed suspension or cancellation, along with a direction to present, within 30 (thirty) days, his reply to the proposed action.

(3) Where a reply is furnished by the licensee pursuant to the notice under sub-section (2), the Commission, upon consideration of such reply, may, with or without condition-

(a) direct necessary corrective measures;

(b) cancel the licence;

(c) suspend the licence for a specified period and direct necessary corrective measures;

(d) direct the payment of an administrative fine not exceeding 3 (three) lac taka and, in an appropriate case, also direct necessary corrective measures; or

(e) take both the actions specified in clauses (c) and (d).

(4) The licensee shall not be entitled to any compensation for damage caused by any action under sub-section (3), nor shall he be entitled to raise such claim before any court or other authority, and even if such claim is raised, the court or other authority shall summarily reject it.

47. Interconnection.- (1) Subject to the provisions of this Act and regulations, an operator may establish interconnection between his telecommunication network with that of another operator.

(2) If, in an area specified by the Commission, 25% of the consumers take service from more than one operator, such operators

shall have the following obligation in respect of interconnection and providing access to the interconnection :

(a) interconnection agreements shall be executed within 3 (three) months from the first day on which the new operator starts providing telecommunication service;

(b) the operators shall execute such agreements among themselves; however, on the application of any operator, the Commission may, in consideration of the existing circumstances, extend the time limit but not exceeding 3 (three) years; and the Commission shall notify, in at least two widely circulated national dailies published from Dhaka, the fact of such decision along with a full explanation of the circumstances;

(c) the real cost in relation to universal service provided by operators of ordinary or cellular mobile telephone service, shall be fixed and paid at a rate as mutually agreed among the operators; and the Commission may, keeping in view of the particular circumstances, also specify that the operators providing other services shall comply with the cost so fixed in relation to the universal service; and if they fail to agree on such rate, the Commission may fix the rate which shall be followed in making payment of the cost, provided such cost is part of the total cost of interconnection;

(d) in determining the terms and conditions of interconnection, the operators shall act in a non-discriminatory and transparent manner;

(e) copies of interconnection agreements shall be delivered to the Commission and interested parties;

(f) charges realizable for the use of interconnection shall be fixed by way of adjusting the actual cost and a reasonable rate of profit from the investment in interconnection; and the manner of fixation of such charge shall be transparent;

(g) the operators shall keep a separate account for each interconnection so that all the heads of expenditure for the interconnection and the income there from may be specifically identified.

(3) The Commission-

(a) may direct any operator to present his cost of interconnection and the justification for charges for the interconnection services;

(b) shall ensure adequate number of interconnections for the purpose of protecting the interests of consumers;

(c) shall publish a directory containing model interconnection agreements and guidelines.

(4) Where the interested parties, or the persons, who under sub-section (2) are bound to execute interconnection agreement, cannot agree on the terms of such agreement, any of them may present the matter to the Commission, or on its own motion, the Commission may take up the matter, and determine the terms of the agreement as it considers appropriate.

(5) In appropriate cases, the Commission may, on its own motion-

(a) interfere with any matter relating to interconnection of any operator, for the purpose of ensuring public interest;

(b) direct the concerned parties to an existing interconnection agreement to amend the terms thereof;

(c) specify the time-limit for holding discussion and finalising a proposed interconnection agreement;

(d) take action against establishing or maintaining a monopoly created by way of interconnection.

CHAPTER VI

Tariff, Charges etc.

48. Approval of tariff.- (1) An operator shall, before providing service, submit to the Commission a tariff containing the maximum and minimum charges that may be realized for such service, and until the tariff is approved by the Commission, the operator shall not start providing the service or realizing charges for the service.

(2) While submitting a tariff under sub-section (1), the operator shall also furnish the justification therefor .

(3) Where the Commission approves the tariff, it shall publish the approved tariff in such form and in such manner as it may specify in this behalf, and may also include additional information if considered necessary.

(4) Within 60 (sixty) days after a tariff is submitted, the Commission shall-

(a) approve the tariff with or without modification, or substitute an alternative tariff, or direct the operator to submit an alternative tariff;

(b) reject the tariff within the said 60 (sixty) days and shall, within 15 (fifteen) days of the rejection, inform the operator of such decision and the reasons therefor ; or

(c) if it does not take a decision under clause (a) or (b), publish, within the said 60 (sixty) days or within the next 15 (fifteen) days, the fact of no-decision for public information, and shall also specify the time-limit within which it intends to take decision; and such delay shall not exceed 60 (sixty) days.

49. Principles of determination of tariff by Commission.- (1) The Commission shall, in determining or approving a tariff, follow the general principles as specified below:-

(a) the tariff shall be fair and reasonable;

(b) the charges shall be equally applicable to the various persons providing a particular service or to the persons taking that service;

(c) if an operator provides more than one service, but there exists competition in the market in providing one of such services and no competition in case of another service provided by him, then-

(i) subsidy from the earnings of the service which is subject to competition shall not be allowed for the other service which is not subject to competition;

(ii) the arrangement, if any, existing at the commencement of this Act, for providing subsidy from the earning of the service which is not subject to competition shall be progressively abolished within the time-limit specified by the Commission;

(d) no person or group or class shall, in respect of tariff or charges for a service, be given undue preference or be subjected to discrimination or disadvantage.

(2) The Commission may, in determining whether a tariff is fair and reasonable, adopt any clear and reasonable method, and such method may be based on the return of an operator or other information.

(3) Where, in relation to a service provided by an operator, the Commission is of opinion that-

(a) an activity of an affiliate under the operator is integral part of that service ; and

(b) the provisions of this Act or regulations are not sufficient for ensuring that the rate of charges fixed by the operator for the

services are fair and reasonable, the Commission may consider the income or part thereof earned by the affiliate from the said activity is the income of the operator.

50. Discriminatory charges prohibited.- (1) An operator shall not, in relation to a service provided by him or the charges for such service, make any discrimination or create any inconvenience to any person or group or class, nor shall he give any unfair or unreasonable preference to himself or any other person.

(2) Where allegations of making discrimination, creating inconvenience or giving preference are brought against an operator-

(a) the Commission shall, within 15 (fifteen) days of the receipt of the allegations, serve a 15 days' notice on the operator directing him to submit his reply to the allegations, if the Commission considers that the said allegations are prima facie justified;

(b) the burden of proof that his conduct was not discriminatory against, or preferential or did not create any inconvenience to, any person shall lie on the operator;

(c) the Commission shall, in accordance with sub-section (3), take necessary action after consideration of the allegations brought against, and the reply submitted by, the operator.

(3) Where an operator contravenes sub-section (1), the Commission may impose on him an administrative fine not exceeding 50 (fifty) thousand taka or, in an appropriate case, direct the operator to pay to the affected person a compensation not exceeding 50 (fifty) thousand taka, or direct the operator to refrain from the discriminatory conduct, or the Commission may take all or more than one of such actions.

CHAPTER VII

Standard of telecommunication apparatus and service

51. Standards of telecommunication apparatus.- (1) Subject to sub-section (4), the Commission may specify the national standards and technical aspects of the apparatus that are used in a telecommunication system and in providing telecommunication services.

(2) For the purposes of sub-section (1), the Commission-

(a) may, for different class of apparatus, determine different standards, criteria and method for verifying their compliance;

(b) shall publish a notice in the official Gazette and two national dailies that it intends to determine such standard, criteria and method and, invite comment or suggestion on the standards, criteria and method proposed in such notice and shall also specify the date since when such standards, criteria and method shall be effective;

(c) shall, upon consideration of the comment or suggestion, if any, received under clause (b), finalise the standards, criteria and method, and also publish them in the same manner;

(d) may determine the standards of radio method and interference causing apparatus and technical conditions applicable thereto.

(3) In determining the standards, criteria and the method for verifying their compliance, the Commission shall be guided by the needs for a safe, modern and efficient telecommunication service and interconnection.

(4) The Commission shall not, before determining under this section the standards, criteria and related conditions of licence, impose any restriction as to whether or not any apparatus manufactured by a company or other enterprise may be used in providing a service for which licence is necessary.

52. Technical standards etc. of terminal apparatus.- (1) The Commission shall, form time to time, make and publish, a directory wherein the names and specifications, technical standards and related matters of terminal apparatus shall be specified. (2) Every person shall follow the directory in manufacturing, importing and marketing terminal apparatus and installing them in a telecommunication system.

53. Search etc. for harmful interference.- (1) It shall be lawful for the Commission to search out harmful interference, and where the Commission finds that a person has in his possession or control interference causing radio apparatus or other apparatus, it may order the person to stop the operation of that apparatus or to repair or substitute the apparatus within a time specified in the order, so that the interference may not be caused any more.

(2) A person commits an offence if he contravenes an order under sub-section (1) or fails to comply with such order, and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 3 (three) years or to a fine not exceeding 3 (three) lac taka or to both.

(3) Where an information is obtained with the help of electronic or other device used in the monitoring or surveillance activities for finding out harmful interference and such information is printed on a document under the signature of an authorized officer of the Commission or is attested by that officer, the information shall be admissible as evidence in any proceedings of the Commission or a Court.

54. Determination of the standards of telecommunication.- (1) The Commission may, by making regulations or by publishing notice at least in two widely circulated national dailies, determine the standards of various telecommunication services, and in providing those services, the operators shall be bound to follow those standards.

(2) Where a standard is determined under sub-section (1), the Commission shall, from time to time, take steps for publicity of the standard so that the people get opportunity to know about it.

CHAPTRE VIII

Radio communication and spectrum management

55. Necessity for licence for radio apparatus, authority, procedure etc.- (1) No person shall, without a licence, establish, operate or use a radio apparatus for the purpose of radio communication in the land or territorial waters of Bangladesh or in the space above them, nor shall he use any radio frequency other than the frequency allocated by the Commission.

(2) The Commission shall have the exclusive authority to issue licence and to allocate the radio frequency under sub-section (1).

(3) The manner of issuance of licence, allocation of frequency, and their renewal, suspension and cancellation, the qualifications and disqualifications of a licensee, the licence-fees and other related matters shall be determined by regulations, and until regulations are made, general or special resolutions of the Commissions shall be applicable to those matters.

(4) A licence issued or a frequency allocated under this section or the right to use such licence or frequency shall not be transferable, and if any such transfer takes place it shall be void.

(5) Clause (i) of section 37(3) shall be applicable to such licence.

(6) No licence under sub-section (1) shall be required in the following cases:-

(a) installation, operation or use of a radio apparatus by the Police, Bangladesh Rifles, Coast Guard, any of the defence forces or any other security force to meet its own requirement;

(b) installation, operation or use of a radio apparatus by the Ministry of Foreign Affairs or an intelligence agency of the Government to meet its own requirement;

(c) installation, operation or use of a radio apparatus in a battle-ship or defence air-craft or in other vehicles used for the affairs of the State : Provided that no radio frequency other than the frequency allocated by the Commission shall be used in such radio apparatus.

(7) A person commits an offence if he, in violation of sub-section (1), installs, operates or uses any radio apparatus without a licence issued by the Commission or if he uses a radio frequency without getting allocation from the Commission; and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 10 (ten) years or to a fine not exceeding 10 (ten) lac taka or to both, and if the offence continues, he shall be liable to an additional fine not exceeding 20 (twenty) thousand taka for each day of the continuous period after the first day.

56. Spectrum Management Committee.- (1) For the purpose of management of radio frequency, the Commission shall, as soon as may be after commencement of this Act, form a committee to be known as the Spectrum Management Committee, hereinafter referred to in this Chapter as the Committee.

(2) The Committee shall consist of one Commissioner and such number of other members as the Commission may specify, and the Commissioner shall be the President of the Committee.

(3) As soon as the Committee is formed, the Commission shall inform the Ministry of such formation; and the Ministry shall take all necessary steps for transferring to the Committee the overall functions and responsibilities of the Frequency and Wireless Board including the documents related to allocation of radio frequencies made prior to the commencement of this Act, the pending applications for allocation of radio frequency and all related matters; after such transfer the said Board shall stand dissolved.

(4) Subject to any general or special instruction of the Commission, the Committee may determine the manner and other matters of holding of meetings, carrying on its activities and making of recommendations and decisions.

(5) Subject to the other provisions of this Chapter, the functions of the Committee shall be as follows :

(a) to make recommendation to the Commission on the principles of allocation of radio frequency and fixation of fees for such frequency;

(b) to make recommendation to the Commission for specifying the radio frequencies to be used for operating radio apparatus or for providing services by various licensees, broadcasting enterprises and other organizations ;

(c) to make recommendation to the Commission on the methods and time-limits of allocation of radio frequencies and the revocation or modification thereof;

(d) to co-ordinate the international and multipurpose use of radio frequency and to frame policies thereon, to present such policy for approval of the Commission and to revise from time to time the policies approved by the Commission;

(e) to revise matters relating to radio frequency band in order to ensure their proper use and receipt of better information by using such band;

(f) to determine the technical standards applicable to radio apparatus or interference causing apparatus; and to make recommendation on the issuance of technical acceptance certificates;

(g) to make recommendation on the issuance of licence for radio apparatus;

(h) to monitor the compliance of the provisions of this Act and regulations in respect of the use of the allocated radio frequency spectrum, and to make suggestions on the actions to be taken, if any.

(6) The Commission may direct the Committee to perform functions other than those mentioned in sub-section (5).

(7) In exercising powers, performing functions and duties under sub-section (5), the Committee shall follow the applicable criteria specified or recommended by the International Telecommunication Union or by its concerned Standing Committee or by other organization.

(8) For getting a radio apparatus licence, allocation of a radio frequency or technical acceptance certificate, an application shall be submitted to the Commission; and within 7 (seven) days of the receipt of

such application, the Commission shall send it, with comments, if any, to the Committee which shall, within the next 30 days, make such inquiry on the matter as it considers necessary and present the application with its comments and recommendations to the Commission.

(9) The Commission shall, after consideration of the comments and recommendations of the Committee on the concerned application, take decision on the issuance of a licence for radio apparatus or, as the case may be, a technical acceptance certificate or allocation of radio frequency; and shall in all cases determine the conditions applicable thereto after consideration of the Committee's recommendation.

57. Technical Acceptance Certificate.- (1) The Commission may, by issuing notice in at least two widely circulated national dailies published from Dhaka, or by making regulations, specify the radio apparatus or interference causing apparatus for which technical acceptance certificate is necessary.

(2) When a technical acceptance certificate in relation to an apparatus is required by a notice published, or by regulations made, under sub-section (1), no person shall, except in accordance with such certificate, use, distribute, sell or offer for sale, lease out or demonstrate that apparatus.

(3) A person commits an offence if he violates sub-section (2), and for such offence he shall be liable to imprisonment for a term not exceeding 5 (five) years or to a fine not exceeding 5 (five) lac taka or to both.

(4) The Commission shall, in relation to an apparatus mentioned in subsection (1),-

(a) make regulations on the standards determined by the Spectrum Management Committee under section 56(5)(f) or publish such standards in at least two widely circulated national dailies; or

(b) make regulations specifying the procedure and other matters relating to the issuance of a technical acceptance certificate, and renewal, suspension and cancellation thereof, and until such regulations are made, those matters shall be determined by administrative orders.

(5) A technical acceptance certificate issued under this section shall remain valid for the period specified therein and may be renewed after the expiry of that period.

(6) The procedure for issuance of a technical acceptance certificate and the renewal, cancellation and suspension thereof and the fees therefore shall be determined by regulations, or until regulations are made, by administrative orders of the Commission.

58. Monitoring and control of emission of electro-magnetic energy.- The operator shall monitor the emission of all kinds of electro-magnetic energy in the lands and territorial waters of Bangladesh and the space above them, and shall control the harmful effect of such emission, and for that purpose it may issue necessary direction to any person or body.

CHAPTER IX

Receipt and disposal of consumer-complains

59. Provisions relating to receipt and disposal of consumer-complains.- (1) Every operator providing telecommunication service shall establish sufficient number of complain-centres so that he can collect information on the inconvenience or complain of the consumers in respect of that service or related matters, and shall, form time to time, publish notice about the location of, and communication with, such centres.

(2) Any consumer may, by telephone message or written complaint, present his inconvenience or complain.

(3) All information relating to the complains received from consumers and disposal of such complains shall be recorded in a register.

(4) On receipt of an information or complain about the inconvenience of a consumer, the service provider shall immediately take necessary action and shall follow the code of practice framed in this behalf by the Commission.

(5) Where the service provider, after being informed of an inconvenience or complain of a consumer, fails to timely and properly resolve the inconvenience or the complain, that consumer may in writing apply to the Commission for taking necessary action on the matter.

(6) Within 7 (seven) days of receipt of such application, the Commission may, after necessary inquiry, give proper directions to the service provider to take necessary steps for resolving the said inconvenience or complain.

(7) If the direction under sub-section (6) is not complied with, the Commission may, under section 63, issue a compulsory enforcement order.

CHAPTER X

Inspection and Compulsory Enforcement

60. Appointment of Inspector.- The Commission may, for the purposes of this Act, appoint any of its officers as an Inspector.

61. Powers of Inspector.- (1) For implementing the provisions of this Act, an Inspector may, subject to sub-section (3)-

(a) enter any place at any reasonable time, if he has reason to believe that

(i) a radio apparatus or an interference causing apparatus not permitted under this Act has been kept or is being used in that place; or

(ii) a telecommunication system or a telecommunication apparatus not permitted under this Act has been kept in that place; or

(iii) a telecommunication service is being provided or a radio apparatus has been installed or is being operated in that place without necessary licence or permit or in violation of a condition thereof;

(b) examine such apparatus, if found;

(c) examine any log book, report, data, record, bill or any other document found in that place, if he, on reasonable grounds, believes that such examination is necessary for implementation of any provision of this Act or regulations or any direction or directive of the Commission, and he may take copies or photocopies of the whole or part of the document, or may also take necessary extract from it;

(d) inquire the occupier or user of, or the person having control over, the said system or apparatus, and may arrest him and also seize the apparatus if the inspector believes that the said occupier, user or person having control may abscond or, as the case may be, the apparatus may be removed or destroyed;

(e) recommend to the Commission for seizure of an apparatus which is not permitted for use in a particular telecommunication system or for providing a particular service.

(2) The Commission may, upon consideration of the recommendation made under sub-section (1)(e) seize the said apparatus, and if the apparatus so seized is not apparently owned by any person, it shall vest in the Commission, and if, within 60 (sixty)

days of such seizure, any person claims ownership of the apparatus, the Commission may, after necessary inquiry, return it to the claimant or take such other action as it considers appropriate.

(3) If the place mentioned in sub-section (1) is a dwelling house of any person, the Inspector shall not enter that place without the consent of the person in charge thereof; however such consent shall not be necessary in the following cases:-

(a) if an warrant has been issued by a Magistrate under sub-section (4); or

(b) if special circumstances exist wherein procurement of warrant is not practicable.

Explanation : For the purposes of this sub-section, any circumstances shall be deemed to be special circumstances, if the act of procuring the warrant is likely to endanger the security of life, property or evidence of an offence or to allow the destruction or removal of any evidence of an offence.

(4) If, from the report of an Inspector, or from an information furnished by any other person along with a verified statement as to the truth thereof, it appears to the Magistrate that-

(a) for the purpose of performing the functions and responsibilities of the Inspector under this Act, entry to a dwelling house is necessary; and

(b) consent to the said entry has been refused or that there are reasonable grounds to believe that such consent will be refused ,then a Magistrate of the first class or a Metropolitan Magistrate for a metropolitan area may, on the application of the concerned Inspector, issue a warrant authorising the Inspector to enter into that house and, in a proper case, to apply force, and the Magistrate shall mention the name of the Inspector in such warrant and may, if he considers appropriate, specify any condition therein.

(5) In executing an entry to a dwelling house authorised under sub-section (4), the Inspector shall not apply force, unless he is accompanied by police force.

(6) Where an Inspector enters any place, the occupier or the person in charge thereof shall render all reasonable assistance to, and furnish all information required by, the Inspector so that he can perform his duties under this Act.

(7) No person shall, during the time an Inspector carries on his duties under this Act-

(a) resist the Inspector or wilfully create any obstruction; or

(b) knowingly present to the Inspector a false or misleading information, whether verbal or written;

(8) A person commits an offence if he violates the provisions of sub-section

(7), and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 3 (three) years or to a fine not exceeding 3 (three) lac taka or to both.

62. Prima facie truth of Inspector's certificate or report.- (1) Where a certificate or report containing the results of an examination or inspection under this Act purports to be signed by an Inspector, that certificate or report shall be admissible as evidence in a proceedings under this Act, and, unless the contrary is proved, the contents of the certificate or report shall be considered as proof of such examination or report.

(2) The Commission shall, before initiating a proceeding in the court under this Act on the basis of the said certificate or report, send a copy thereof to the accused person personally or to his last known place of work or residence.

(3) In such proceedings, the accused person may apply to the court for a direction to the Inspector to appear before the court so that the accused person gets an opportunity to cross-examine him.

63. Issue of enforcement order and penalty for its violation.- (1) If a licensee or the holder of a certificate or permit-

(a) violates any provision of this Act or regulations or any condition of the licence or permit in operating a system or in providing a service; or

(b) has procured the licence or permit or technical acceptance certificate by furnishing a false information, the Commission may direct the licensee or the holder of the permit or certificate to show cause within 30 (thirty) days as to why an enforcement order shall not be issued or why the licence or permit or certificate shall not be cancelled.

(2) A notice under sub-section (1) shall contain specific description of the nature of the violation and the corrective or remedial measures, if any.

(3) Where, in response to the notice under sub-section (1), any reply or any satisfactory explanation in respect of the allegations made in the notice, is not submitted to the Commission, or the corrective or remedial measures directed by the Commission are not taken within the time specified in such notice, the Commission may, after recording reasons, by an order-

(a) impose upon the violator an administrative fine not exceeding 3 (three) lac taka and, if the violation continues after the issuance of the order, an additional administrative fine not exceeding 30 (thirty) thousand taka for each day; and

(b) in a proper case, suspend or cancel the licence, permit or certificate or impose additional conditions.

64. Commission's power to issue injunction on current or probable violation.- (1) Where the Commission is of opinion that a person is acting or about to act in a manner that has or will have the effect of violating the provisions of this Act or regulations or any condition of a licence or permit or a direction or directive of the Commission, it may, by a written notice, direct that person to show cause within 7 (seven) days as to why he shall not be restrained from such act, and if any cause is shown by him, the Commission may, after considering it, direct him to refrain from such act or may give such other direction as it considers appropriate in the circumstances : Provided that, if the Commission is satisfied that the violation or probable violation is of such a nature that the person should be immediately restrained from such act, the Commission may, at the time of issuing the notice, pass an interim order directing that person to refrain from the violation or the concerned act till the matter is decided by the Commission.

(2) The person to whom a direction is issued under sub-section (1) shall properly comply with the direction or, the as case may be, refrain from the concerned act.

(3) If a person violates sub-section (2), the Commission may impose upon him an administrative fine not exceeding 1 (one) lac taka, and the person commits offence if he fails to pay the fine, and for such offence he is liable to be sentenced to imprisonment for a term not exceeding 3 (three) years or to a fine not exceeding 3 (three) lac taka or to both.

65. Administrative fines.- (1) The Commission may, in addition to the administrative fines specified in this Act, make regulations for imposition of such fine for violation of the other provisions of this Act

or regulations : Provided that administrative fines shall not be so provided for violation of sections 35(1), 55(1) and 57(2).

(2) Where an administrative fine may be imposed for violation of any of the provisions of this Act or regulations, the Commission shall serve on the violator a notice to the effect that he may admit the violation, deposit the administrative fine specified in the notice and thus get himself discharged from the liability, and that he may also explain his position in this regard.

(3) In relation to the violation mentioned in sub-section (2)-

(a) an Inspector shall fill in the prescribed notice specifying therein the relevant facts and put his signature thereon and shall-

(i) serve the notice personally to the accused person, or

(ii) send the notice to the last known address of his residence or place of work ;

(b) the inspector shall specify in the notice the various aspects to be considered in respect of the alleged violation and the procedure to be followed, and also the amount of administrative fine that may be imposed;

(c) the accused person may-

(i) admit the violation and pay the administrative fine specified in the notice;

(ii) admit the violation and request for reducing the said fine by explaining the circumstances in which the violation took place; or

(iii) deny the violation and in support of such denial furnish the explanation and necessary information and request for discharge from the liability of the proposed fine.

(4) Where an application is submitted under sub-clause (ii) or (iii) subsection (3)(c), the concerned officer of the Commission authorized in behalf shall consider the matter as a whole and record his decision along with reasons and shall, within 3 (three) days of the decision, deliver to the applicant a copy thereof.

(5) The accused person may, within 15 (fifteen) days of the decision under sub-section (4), apply in writing to the Commission for review of the decision and the Commission shall, within 30 (thirty) days of lodging the application, dispose of the matter after giving the applicant a reasonable opportunity of being heard.

for a term not exceeding 3 (three) years or to a fine not exceeding 3 (three) lac taka or to both.

68. Penalty for misuse of radio or telecommunication apparatus by employee.- (1) An employee of an operator shall not-

(a) intentionally transmit, by using a telecommunication apparatus or radio apparatus, a message which to his knowledge is false, or misleading, or is likely to affect the efficiency of a telecommunication service or the security of life or property of a person;

(b) in course of his duty -

(i) use any telecommunication apparatus or radio apparatus with intent to obtain any information relating to the sender or addressee, or the content of, a message sent by telecommunication or radio communication, unless the Commission has authorized that employee or the operator to receive the message;

(ii) except for the requirement of a legal proceedings of the Commission or a court or of a consequential proceeding, disclose any information about the sender or addressee or contents of a message which has come to his knowledge only by using or in connection with the use of a telecommunication apparatus or radio apparatus;

(c) create obstruction in any part of a telecommunication network which is being used for sending or receiving an information or message or anything else, nor shall he obtain any information relating to the sender or addressee or content of the message, unless he is authorized in this behalf by the Commission or by the sender or addressee of such message.

(2) A person commits an offence if he contravenes sub-section (1) and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 5 (five) years or to a fine not exceeding 5 (five) lac taka or to both.

69. Penalty for sending obscene, indecent message etc.- If-

(a) a person offers to another person engaged in the operation of a telecommunication apparatus or radio apparatus to send an obscene, threatening or grossly insulting message , or

(b) the person secondly mentioned, pursuant to such offer, knowingly or intentionally sends that message, then, in case of clause (a), the person offering to send, and in case of clause (b), both the person offering to send and the person sending, the message commits an offence, and for such offence the person so offering to send or, as the case may be, the person sending the message shall be liable to be sentenced to imprisonment for a term not exceeding 6 (six) months or to a fine not exceeding 50 (fifty) thousand taka or to both.

70. Penalty for causing annoyance by telephone calls.- (1) A person commits an offence if he, without a reasonable excuse, repeatedly makes telephone calls to another person in such a manner that the calls cause annoyance or inconvenience to that other person, and for such offence the firstly mentioned person shall be liable to be sentenced to a fine not exceeding 25 (twenty five) thousand taka and, in default of payment of fine, to an imprisonment for a term not exceeding 3 (three) months.

(2) It shall be lawful for the operator, upon a complaint and authorization in this behalf from the person to whom such calls are made or from another person on behalf of the firstly mentioned person, to trace the source of, to intercept, monitor or record the calls or to take steps to prevent the calls.

71. Penalty for eavesdropping telephone conversation.- A person commits an offence, if he intentionally listens to a telephone conversation between two other persons, and for such offence, he shall be liable to be sentenced to imprisonment for a term not exceeding 6 (six) months or to a fine not exceeding 50 (fifty) thousand taka or to both.

72. Penalty for trespass, unlawful stay, causing damage to apparatus, obstruction to operation activity etc.- A person commits an offence, if he-

(a) without permWission of the person-in-charge, enters an office where telecommunication or radio communication is operated with the help of licensed telecommunication apparatus or radio apparatus;

(b) after entry to that office in any way, fails to leave it even after the request of the person in-charge or of a person subordinate to the person in-charge;

(c) ignoring a prohibitory notice, enters a place where such apparatus has been kept;

(d) after entry to such office or place in any way, obstructs any person to perform his duty; or

(e) internationally causes damage to such apparatus, or removes it, or unlawfully impairs the efficiency of it or renders it unworkable , and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 7 (seven) years or to a fine not exceeding 7 (seven) lac taka or to both.

73. Other offences and penalties.- (1) Any of the following acts of a person shall be an offence, namely:-

(a) the act of operating a telecommunication system or providing service in violation of any condition of a licence or permit, or any abetment of such violation;

(b) the act of sending or receiving any information or providing any service by using a telecommunication system or radio apparatus which that person knows or has reason to believe that such system or apparatus has been, in violation of this Act, established or being operated under his direct or indirect control, or the act of using such system or apparatus for any purpose incidental to the aforesaid sending or receiving of information or providing service;

(c) the act of using any mechanical, electrical or other device in order to avoid charges payable for a service taken or to be taken;

(d) while performing duties in a licensed telecommunication network, the act of intentionally causing any change in, or distortion of, or unlawful interference to, the contents of a message sent through that network;

(e) failure or refusal to supply to the Commission an information or document which the Commission is entitled to obtain under this Act or regulations and for the supply of which the Commission has given 10 days' notice.

(2) Where a person is found guilty of an offence under sub-section (1), he shall be liable to be sentenced to imprisonment for a term not exceeding 5 (five) years or to a fine not exceeding 5 (five) lac taka or to both; and if such offence is a continuous one, he shall be liable to an additional fine not exceeding 25 (twenty five) thousand taka for each day of the continuous period after the first day.

(3) Where a person contravenes a provision of this Act or the regulations made there under for which no penalty is prescribed in this Act or the regulations he shall, on being found guilty of that violation, be liable to be sentenced to the following penalties :-

(a) for the first-time violation, imprisonment for a term not exceeding 2 (two) years or to a fine not exceeding 2 (two) lac taka or to both;

(b) for each subsequent violation to a fine not exceeding 3 (three) lac taka or an imprisonment for a term not exceeding 3 (three) years or to both.

(4) The imposition of a penalty under sub-section (2) shall not affect any other right or remedy of a person aggrieved by the concerned offence.

74. Penalty for abetment of offence etc.- If a person aids the Commission of any offence under this Act, or if he instigates or conspires to commit such offence and the offence is committed as a result of that instigation or conspiracy, he shall be liable to be sentenced to the same penalty prescribed for the commission of that offence.

75. Provision in regulations relating to offence, penalty, compensation.- The Commission may make regulations on the following:-

(a) identifying the conditions of a licence or permit issued by the Commission or certain provisions of regulations the violations of which will constitute offence and imposition of a penalty of imprisonment for a term not exceeding 2 (two) years or fine not exceeding 2 (two) lac taka or both for such offence ;

(b) specifying the compensation, which may extend to 2 (two) lac taka, to be paid to a person affected by the violation of regulations or the conditions of a licence or permit issued by the Commission, and the procedure for realization of such compensation.

76. Offence by company.- (1) If the person contravening a provision contained in or made under this Act is a company, every owner, director, manager, secretary or other officer or employee or representative of the company shall be deemed to have violated that provision, unless he proves that the violation took place beyond his knowledge or that he took all possible steps within his capacity to prevent the violation.

Explanation.- In this section -

(a) "company" means any company, statutory body, partnership, society or association of persons;

(b) "director" includes a partner, or a member of a board of director, by whatever name called.

(2) Notwithstanding the provisions of the Criminal Procedure Code, where an offence under this Act or regulations is committed by a company, the Court of Sessions, having jurisdiction over the place at which the registered office, or the head office of the company is situated or, if the company does not have such an office, the place from which its activities are generally regulated, or the place at which the offence has been committed or the concerned offender of the company is available shall be the court of competent jurisdiction.

77. Jurisdiction of courts relating to cognizance and trial of offences.- (1) Notwithstanding the provisions of the Criminal Procedure Code, no court inferior to a Court of Sessions shall be competent to hold the trial of an offence under this Act or regulations.

(2) Only a Magistrate of the first class or a Metropolitan Magistrate or a court superior to such Magistrate shall be competent to take cognizance of an offence under this Act on the basis of a report of an Inspector or a person authorized by the Commission.

Explanation.- Despite the fact that a person has not been sent by such Magistrate, the Court of Sessions may on the basis of that report or related information, take cognizance of an offence which appears to have been committed by that person.

(3) Where the said court takes cognizance of an offence, it may take all actions in accordance with the Criminal Procedure Code for making the case ready for trial including issuance of summons or warrant arrest for appearance of the accused person in the court.

78. Lodgment of complaint and procedure of investigation.- (1) The Commission may authorize an Inspector or any other officer to investigate an offence specified in this Act or regulations.

(2) The Inspector or the other officer, hereinafter referred to as the investigating officer, may, in view of a complaint of any person or other information, initiate proceedings under this section.

(3) Before starting formal investigation of an offence, the investigating officer shall submit to the officer specified in this behalf by the Commission a preliminary report and the secondly mentioned

officer shall, upon consideration of the relevant facts and circumstances, decide, within 7 days of the submission of the report, as to whether or not formal investigation or other action under this Act or regulations or no such action in relation to the matter will be expedient, and accordingly subsequent actions shall be taken.

(4) Where a decision to initiate formal investigation is taken under subsection (3), the investigating officer shall present to the concerned police station a copy of the said preliminary report which shall be recorded in the police station as information relating to the offence.

(5) The investigating officer shall, in relation to the investigation of an offence, be competent to exercise the same powers as the officer-in-charge of a police station can exercise.

(6) After completion of the investigation, the investigating officer shall submit to a Magistrate of the first class or to a Metropolitan Magistrate having jurisdiction the original copy of the investigation report and also the supporting documents or copies thereof; and shall keep a copy of the report at his office and send another copy to the police station.

(7) Despite the provision of sub-section (3), the investigating officer may, if the relevant offence and the circumstances thereof so require, seize any relevant document, thing or apparatus before receipt of a decision infavour of holding formal investigation under that sub-section, if he is satisfied that any delay may result in the destruction or removal of the document, thing or apparatus, and he may also arrest any person involved in the offence, if he is satisfied that such person is likely to abscond.

79. Application of Criminal Procedure Code.- (1) Subject to the provisions of this Act, and the rules and regulations made thereunder, the Criminal Procedure Code shall apply to the investigation of an offence under this Act, trial, appeal and all incidental matters.

(2) A case initiated in a court on the basis of a report of an Inspector under this Act shall be deemed to be a case so initiated on the basis of a police report.

80. Assistance to Public Prosecutor etc. by officer of Commission.- An officer of the Commission specified in this behalf may assist the Public Prosecutor or the concerned Additional or Assistant Public Prosecutor in conducting a case under this Act in the Court of Sessions, and that officer may himself make submission before the Court.

81. Confiscation of apparatus etc.- (1) Where an offence under this Act is committed, the Court may, in consideration of the nature and the circumstances of the offence, pass in favour of the Commission an order of confiscation of the telecommunication apparatus or radio apparatus or the vehicle or other thing or document, in this section referred to as the materials, in relation to or with the help of which the offence has been committed : Provided that the materials of a Government organization or a statutory body shall not be so confiscated in connection with commission of any such offence.

(2) Where any material is confiscated under sub-section (1), the Commission shall publish in two widely circulated national dailies published from Dhaka a notice about such confiscation; and after 30 (thirty) days of publication of the notice, the Commission may dispose of the confiscated material.

(3) If any person, not being the person found guilty of the offence, claims any interest in the confiscated materials as an owner, mortgagee, lien holder or in any other capacity, he may, within 30 days after publication of the notice of confiscation, submit to the trial court an application, hereinafter referred to as the said application, for obtaining an order under sub-section

(5); and the court shall fix a date for hearing on the said application.

(4) The applicant shall, at the time of or before submission of the said application, send a notice along with a copy of the said application to the Commission and other persons who, to the knowledge of the applicant, claim any interest in the confiscated material under sub-section (3).

(5) If, after giving to the Commission, the applicant and other claimants a reasonable opportunity of being heard, the court is satisfied that-

(a) the offence, in connection with which the materials have been confiscated, was committed beyond the knowledge or permission or consent of the applicant or the other claimant; and

(b) the applicant or the other claimant took such precautionary measures that he had reason to remain satisfied that the offence would not be committed by the permitted possessors or users of the materials, then the court may, declare that the interest of the applicant or other claimant in respect of whom the court is so satisfied will have preference to those of other interested persons; and in addition, the court may direct that the materials be returned to such interested person or persons or, where the materials have been sold or otherwise disposed of, direct the payment of such money out of the sale proceeds to each of such interested persons in proportion to their interest, as the court may consider appropriate.

(6) The said owner or interested person shall not be entitled be to claim any compensation in a proceeding of confiscation or disposal of the material under this section or in any other related proceedings, nor shall he raise any claim for compensation or other claim in any other court.

82. Disposal of realized administrative fine and the fine for commission of offences.- All administrative fines and the fines for commission of offences realized under this Act and regulations shall be credited to the public accounts of the Republic.

83. Right to civil suits and other remedies for unlawful disclosure of message.- (1) If a person, on reasonable grounds, believes that a message sent or received by him has been or will be unlawfully disclosed, or that it has been or will be used in violation of the provisions of section 67(1) or 68(1), he may, for prohibiting such disclosure or use or for realizing compensation from the person liable for such disclosure or use, file a civil suit in the court of Sub-Judge against the person so disclosing or using; and in such a suit the court may pass on order of injunction or award compensation or other relief as it considers appropriate.

(2) If a person has been found guilty of an offence under section 67(1) or 68(1) and if, on the basis of the same occurrence, a civil suit is filed under sub-section (1), of this section, the certified copies of the evidence admitted in the criminal proceedings may be presented for admission in the civil suit to prove the alleged unlawful disclosure or use of a message; and the decision by which that person was found guilty shall, in relation to the relief prayed for, be deemed to be sufficient proof.

(3) A civil suit under sub-section (1) shall be filed within 3 (three) years from the date on which the cause of action for the suit arose.

(4) Filing of a civil suit by a person under this section shall not affect the exercise of his other rights including his right to seek other remedies.

CHAPTER XII
Flow of information

84. Supply of accounts and information to Commission.- (1) The Commission may issue directions to any operator or class of operators on any of the following subjects:-

(a) for the purpose of ensuring compliance with the provisions of this Act or proper exercise of Commission's power, adoption of any method of identifying the cost of providing telecommunication services and adoption of any internationally recognised accounting method : Provided that such accounting method shall be consistent with the methods prescribed in the Companies Act, 1994; and

(b) for the purpose of implementation of the provisions of this Act, furnishing to the Commission information on such matter, and in such periodic reports or other form or manner as the Commission may specify.

(2) Where the Commission has reasons to believe that, for the purposes of implementation of this Act, it is necessary to collect an information or a document from an operator or other licensee, or from the holder of a permit or certificate or any other person, the Commission may direct him to deliver the information to the Commission and he shall be bound to comply with such direction : Provided that such person shall not be compelled to deliver a document or contents thereof which the person is not bound to deliver to a court in connection with a civil suit; and the burden of proof that he is not so bound shall lie on him.

85. Access to information and confidentiality.- (1) Subject to sub-section (2), the Commission shall ensure that people get opportunity to inspect and to collect copies of all information that the Commission receives in course of performance of its functions under this Act : Provided that the Commission may make exception in case of an information that if considers confidential

(2) No Commissioner, or consultant, officer or employee or any other person employed by the Commission shall knowingly disclose or allow to be disclosed any confidential information to any other person in a manner so that the information may be used to the benefit of that other person or to the detriment of a related person; disclosure of a confidential information shall be deemed to be a misconduct.

Explanation.- This sub-section shall apply to any person who was a Commissioner, consultant, officer or employee of the Commission.

(3) If the Commission, in the course of a proceedings, receives a confidential information and it is of the opinion that the information should be published in the public interest, the Commission may, after giving reasonable opportunity of being heard to a person who purports to be interested in the information, decide to publish or not to publish the information; and in an appropriate case the Commission may itself publish the information or direct the concerned person to publish it.

86. General inquiry and decision thereon.- The Commission may, on its own initiative or on the application of any person, inquire into and take a decision on a matter or activity which is prohibited or permitted or required to be done by this Act.

87. Public hearing and its procedure.- (1) If the Commission, on the basis of an application or other information, is of the opinion that in the public interest a public hearing on a matter relating to the exercise or proposed exercise of its power or on any other matter is necessary, it may hold public hearing.

(2) For the purpose of holding public hearing under sub-section (1), the Commission may form a public hearing committee consisting of three members, hereinafter referred to in this Chapter as the Committee; the Chairman or Vice- Chairman of the of the Commission shall be the president of the Committee, and the two other members shall be appointed by the Commission from amongst the other Commissioners or officers of the Commission.

(3) If the regulations do not specify the procedure to be followed in public hearing, such hearing shall be conducted in the procedure as the Committee may, subject to this Act, consider appropriate.

(4) The Committee shall take decision on any matter on the basis of majority of votes of its members.

(5) The Committee may, for the purpose of obtaining proper evidence or information, require written evidence or arguments on a matter under inquiry and it may also decide on what matter evidence or arguments may be presented.

(6) Where the Committee considers appropriate, it may allow the concerned person to take the assistance of his engaged advocate or expert of the concerned matter or representative in presenting the evidence or information.

(7) The proceedings of a public hearing shall be open to the public, and the president of the Committee shall make arrangements for recording the evidence and other information and the matters considered by the Committee and the minutes of the hearing.

(8) Any person who has been summoned or, although not summoned, any person whose interest is likely to be affected or prejudiced, or any person who has knowledge about the matter under inquiry, may in person or through his authorized representative appear and make submission before the Committee.

(9) The Committee may, during or after completion of the inquiry-

(a) take decision, after recording reasons therefor, on matters under inquiry or any part thereof;

(b) exclude any matter or part thereof from hearing or stop the hearing on it, if it appears to the Committee that such matter or part thereof is trivial or vexatious or unfounded or that further hearing is not necessary or desirable;

(c) generally give all such directions and do all such things as are necessary for ensuring an expeditious and fair hearing on the matter under its consideration and for taking decisions thereon.

(10) The substantial decisions taken under sub-section (9)(a) or summery of such decisions shall be published in at least two widely circulated national dailies, and the copy of each direction issued and decision taken during the public hearing shall, subject to payment of the fees specified in this behalf by the Commission, be supplied to parties who participated in the hearing.

88. Summoning witnesses and producing evidence in public hearing.- (1) The Committee shall have the same powers to summon a witness or any other person presenting evidence in a public hearing as a civil court may exercise under the Code of Civil Procedure, 1908 (Act V of 1908) in relation to the summoning of a witness or production of evidence in that court; and the Committee shall follow that Code in those matters.

(2) Where the Committee is of opinion that a person is able to give evidence on any matter under inquiry under section 87, the Committee may, by issuing a notice, summon that person to appear before it and take his evidence; any person so summoned may be given reasonable expense for appearing in the public hearing.

(3) If a person summoned to appear in the public hearing-

(a) fails, without reasonable excuse, to appear at the time and place mentioned in the notice;

(b) refuses, without a reasonable excuse, to reply any question put to him by the Committee, or intentionally gives a false or distorted information or statement in reply to such question, or intentionally suppress an information relating to the matter under inquiry; or

(c) refuses or, without reasonable excuse, fails to produce the document or information which is in his possession and has been required by the Committee, he shall be liable for the offence of contempt of court for disregarding the decision of the Committee.

(4) Where the Committee is of the opinion that a person has committed an offence mentioned in sub-section (3), the president of the Committee shall send a report to the High Court Division accordingly.

(5) In a proceeding for trial of the offence of contempt of court initiated on the basis of a report under sub-section (4), the report purported to have been signed by the president of the Committee shall-

(a) be admissible as evidence and, unless the contrary is proved, it shall not be required to be formally proved; and

(b) be a prime facie evidence of the facts stated therein and the decision of the Committee on such facts and the truth of such decision.

(6) The contempt of court specified in sub-section (3) shall be tried by the High Court Division in the same procedure as is followed in the case of a contempt of court under the Contempt of Courts Act, 1926 (XII of 1926), and the penalty specified in that Act may be imposed on the accused person mentioned in that report.

CHAPTER XIII

Transitional provisions, transfer of rights and liabilities

89. Certain matters under Act XIII of 1885 and XVII of 1933 to be vested in the Commission.- If, before the commencement of this Act, the Government had executed a licence-agreement, or had issued a licence, certificate or permit under the Telegraph Act, 1885 (XIII of 1885) or the Wireless Telegraphy Act, 1933 (XVII of 1933), and the Commission is authorized by this Act to issue such licence, certificate or permit-

(a) the licence, certificate or permit so issued shall, subject to the provisions of section 90, remain valid as if it were issued by the Commission;

(b) the licence-agreement so executed shall, subject to the provisions of section 90, remain valid as if it were executed by the Commission;

(c) an order, direction or directive, issued or a permission or consent given in relation to such licence, certificate or permit shall remain valid as if the order, direction, directive, were issued or the permission or consent were given by the Commission under this Act;

(d) the name of the Commission shall be substituted for the Government in any civil suit instituted by or against the Government in relation to such licence or licence-agreement or certificate or permit.

90. Existing licences and other authorizations to continue for limited period.- (1) Any person who, on the commencement of this Act, has a right to establish a telecommunication system or to operate or maintain it or to provide telecommunication service by virtue of a licence, licence-agreement, technical acceptance certificate or permit, hereinafter referred to as the said document, may continue the activity specified in the said document for a period not exceeding 12 months from the date of commencement of this Act, and he shall be deemed to be a holder of the said document under this Act.

(2) If the holder of the said document intends to continue the activities allowed by it, he shall, within three moths after the commencement of this Act or before the expiry of the validity period of the said document, whichever is earlier, apply to the Commission along with the original of that document and relevant information for the purpose of obtaining an order under sub-section (3).

(3) If the Commission, after examining the said document and the relevant information, is satisfied that the said document was properly executed or issued in accordance with the laws, rules or regulations in force at that time, and the content or any condition thereof is not inconsistent with this Act, the Commission-

(a) shall issue an order to the effect that the holder of the said document is a holder of a licence or, as the may be, the holder of

a certificate or permit that may be issued under this Act; and for this purpose a licence-agreement shall be deemed to be a licence;

(b) may amend the said document, if it considers that any condition or content thereof is inconsistent with this Act or any new condition or content is be inserted therein; and the said document shall, subject to such amendment, remain valid; and in such a case the Commission shall specify the amendment in that order or any subsequent order.

(4) Until the disposal of an application submitted under sub-section (3), the activities under the said document may be continued.

(5) Where an application under this section is not submitted in relation to the said document or where the Commission is not satisfied about its legality, the Commission shall issue an order to the effect that the said document shall not remain valid since the date specified in the order.

(6) The legality or propriety of an order issued, or any amendment with regard to a condition or content of the said document made, under this section cannot be called in question in any court.

91. Radio frequency allocated before commencement of Act to continue for limited period.- (1) If a person has acquired, before the commencement of this Act, a right to use a radio frequency, he shall within 6 (six) months of such commencement, apply to the Commission for allocation of that frequency; and the Commission shall send to the Spectrum Management Committee for examination of the application and recommendation thereon.

(2) After consideration of all the applications received under sub-section (1) and the relevant information, that Committee shall make such recommendations as it considers appropriate as to whether the same radio-frequency earlier allocated or any other proper radio-frequency or a radio-frequency of a lower or higher range should be allocated to him or any other action should be taken, and the Commission shall take action accordingly.

(3) The Commission shall, within 12 (twelve) months of the commencement of this Act, dispose of all the applications received under this section; and until his application is disposed of, the applicant shall be entitled to use the radio-frequency earlier allocated to him, unless the Commission otherwise cancels or alters the allocation.

92. Approval of pre-commencement tariff.- All tariff, call-charges and other charges that were existing immediately before the

commencement of this Act shall, until changed under this Act, remain valid after such commencement as if they were fixed under this Act.

93. Bangladesh Telegraph and Telephone Board deemed to be licensee.- Notwithstanding the other provisions of this Act or any contrary provision of the Telegraph and Telephone Board Ordinance, 1979 (XII of 1979), the Bangladesh Telegraph and Telephone Board (BTTB) established under the said Ordinance shall, on the commencement of this Act, acquire the status of a licensee, and the same conditions, so far as may be, shall apply to that Board as are applicable to an operator under this Act: Provided that within 1 (one) year from the commencement of this Act, BTTB shall apply to the Commission for a licence : Provided further that until reorganization of the affairs of BTTB is completed, but not later than 3 (three) years, BTTB may continue to apply the tariff, call-charges and other charger for the services provided by it.

CHAPTER XIV
Miscellaneous

94. Public Servant.- The Chairman and other Commissioners, officers and employees, consultants and any other person authorized by the Commission in writing to exercise its power or to perform its functions shall be deemed to be a public servant within the meaning of section 21 of the Penal Code (Act XLV of 1860).

95. Indemnity.- A person, who is affected by any order or direction issued under the provisions of this Act or regulations, or by anything done or purported to have been done in good faith under those provisions or order or direction, shall not be entitled to bring a suit for compensation against the Minster or an employee of the Government or the Chairman or other Commissioner or any officer or employee or consultant of the Commission.

96. Acquisition of radio apparatus, telecommunication system etc.- (1) The Government may in public interest take over possession of a radio apparatus or the place where it is used, any telecommunication system, and all arrangements that are necessary for operating them, continue such possession for any period and keep the operator and his employees engaged on full-time basis or for a particular time for the purpose of operating such apparatus or system.

(2) The owner or the person having control of the radio-apparatus or telecommunication system taken over by the Government shall vacate possession, and the operator or the employees mentioned in that sub-section shall, with faithfulness and due diligence, comply perform their duties according to the direction of the officer authorized by the Government, and shall transmit and receive the signals, calls, and message as directed by that officer.

(3) The Government shall pay proper compensation to the owner or the person having control of the radio apparatus or the telecommunication system taken over by the Government, and if both sides fail to agree on the amount of such compensation, the Government shall refer the matter to the court for disposal, and the District Judge himself or an Additional District Judge subordinate to him may dispose of the matter in the manner prescribed by rules or in the absence of rules, as he considers appropriate, and his decision on the matter shall be final.

97. Preferential right of Government in emergency.- (1) During war declared, or a situation of war created, by a foreign power against Bangladesh, or during internal rebellion or disorder, or in a situation where the defence or other security of Bangladesh or any other urgent state-affair needs to be ensured, the Government shall have preference compared to the operator or any other user in using a radio apparatus or telecommunication system.

(2) If the President declares an emergency, the Government may suspend or amend any licence or certificate or permit issued under this Act, or suspends any particular activity of, or a particular service provided by, an operator, but the Government shall pay compensation for the suspended service or installation.

98. Power to make rules.- For carrying out the purposes of this Act, the Government may, by notification in the official Gazette, make rules consistent with the provisions of this Act.

99. Power to make regulations.- (1) For carrying out the purposes of this Act, the Commission may, by notification in the Gazette, make regulations consistent with this Act and the rules made by the Government.

(2) Within 7 (seven) days of publication of the regulations in the official Gazette, the Commission shall send to the Ministry, a copy of such regulations and the Ministry may, upon examination of the

consistency of the regulations with this Act and the rules, direct necessary amendments to the regulation, and the Commission shall take necessary steps accordingly.

100. Abolition etc. of Project.- Notwithstanding anything contained in any other law for the time being in force or any contract or other document, the technical assistance project named Establishment of Bangladesh Telecommunication Regulatory Commission project or any other project undertaken by the Government before the commencement of this Act for the purpose of establishing the Commission, hereinafter referred to as the Project,-

(a) shall stand abolished on the date specified by the Government; and

(b) upon such abolition all assets, rights, powers and privileges of the Project shall vest in the Commission; and

(c) all officers and employees of the Project shall be deemed to be the officers and employees of the Commission, and they shall remain in the service of the Commission and their salaries, allowances and other conditions of service shall be determined by the Commission : Provided that any such officer or employee may, within 3 (three) months of the abolition of the Project, express his intention not to remain in the service of the Commission and thereupon he shall cease to be in the service of the Commission.

101. Government's power to remove difficulty.- If there is any difficulty arising from any vagueness in any provision of this Act relating to the power and functions of the Commission, the Government may, by notification in the official Gazette and in keeping with the other provision of this Act, clarify or explain that vague provision and give directives on the course of action of the Commission.

102. Publication of Translated English text of the Act.- As soon as may be after the commencement of this Act, the Government shall, by notification in the official Gazette, publish a translation of this Act in English and such translation shall be known as the Authentic English Text of this Act; however in case of conflict between this Act and the said text, this Act shall prevail.

—

ABBREVIATIONS

A	
ADAB	Association of Development Agencies in Bangladesh
AM	Amplitude Modulation
ATM	automated teller machine
ASBO	Anti-Social Behavior Order
ASP	Application Service Provider
AERE	Atomic energy research establishment
B	
BO	Back Orifice
BCC	Blind carbon copy
BTTB	Bangladesh Telegraph and Telephone Board
BTRC	Bangladesh Telecommunication Regulatory Commission
B2B	Business-to-Business
BGMEA	Bangladesh Garments Manufacturers and Exporters association
BIT	Bangladesh Institute of Technology
BARC	Bangladesh Agriculture Research Council
BBS	Bangladesh Bureau of Statistics
BELA	Bangladesh Environmental Lawyers Association
BIDS	Bangladesh Institute of Development Studies
BOU	Bangladesh Open University
BUET	Bangladesh University of Engineering and Technology
BUP	Bangladesh Unnayan Porishad
BBS	Bulletin Board System
BUET	Bangladesh University Engineering and technology
BCC	Bangladesh Computer Council
BCS	Bangladesh Computer Samiti
BIT	Bangladesh Institute of Technology
BdOSN	Bangladesh Open Source Network
C	

Abbreviations

CAN	Campus Area Network
CC	Carbon copy
CMC	Computer-mediated communication
CDMA	Code Division Multiple Access
CTV	Community Television
CATV	Community Antenna Television
CD	Compact Disk
CRBLP	Center for Research on Bangla Language Processing
CMIS	Computer based Management Information System Cyber CR Cyber Regulations Appellate Tribunal
D	
DDoS)	Distributed Denial of Service
DoS	Denial of Service
DMCA	The Digital Millennium Copyright Act.
DCCI	Dhaka Chamber of Commerce & Industries
DLRS	Department of Land Records & Survey
DOE	Department of Environment
DPHE	Department of Public Health & Engineering
DSL	Digital Subscriber Line
DAB	Digital Audio Broadcast
DOS	Disk Operating System
E	
ESIGN Act	Electronic Signatures in Global and National Commerce Act
ETAC	Excise, Taxes and Customs
EDI	Electronic data interchange
EFT	Electronic Funds Transfer
EGIS	Environment & Geographical Information System
EIES	Electronic Information Exchange System
F	
FTP	File Transfer Protocol

FEJB	Forum of Environmental Journalists of Bangladesh
FTP	File Transfer Protocol
FDMA	Frequency Division Multiplexing Access
FM	Frequency Modulation
FRC	Federal Radio Commission
FCC	Federal Communications Commission
G	
GPEA	Government Paperwork Elimination Act
GUI	Graphical user interface (GUI
H	
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
HRD	Human Resource Development
HF	High Frequency
I	
ICT	Information and Communication Technology
IP	Intellectual property
IT	Information Technology
IP	Internet Protocol
ICMP	Internet Control Message Protocol
ISP	internet Service Provider
IGC	Institute for Global Communications
IRS	Internal Revenue Service
ISO	International Standards Organization
ISAC	Information sharing and analysis center
IMAP	Interactive Mail Access Protocol
IRC	Internet Relay Chat
ICECC	Institute of Certified E-Commerce Consultants
IFB	Institute of Engineers in Bangladesh
IUCN	International Union for Conservation
ISPAB	Internet Service Providers Association of Bangladesh
ITU	International Telecommunication Union

IBM	International Business Machine
L	
LAN	Local Area Network
LGED	Local Government Engineering Department
LISU	Library and Information Service Unit
LW	Long Wave
ICDDRB	International Center for Dhiarial Disease Research, Bangladesh
M	
MAN	Metropolitan Area Network
MIS	Management Information System
MW	Medium Wave
MF	Medium Frequency
MOPT	Ministry of Posts and telecommunications
MMS	Multimedia Messaging Services
N	
NIC	Network Interface Card
NATO	North America Treaty Organization
NACPEC	North American Consumer Project on Electronic Commerce
NGO	Non Government Organization
ADB	Asian Development Bank
NRB	Non-Resident Bangladeshi
NTRC	National Telecom Regulatory Commission
NSDP	National Software Development Plan
NDRCN	National Data Resource Centre Network
NII	National Information Infrastructure
NTP	National Telecommunication Policy
O	
OTA	Over-The-Air
OSS	Open Source Software
P	
PAN	Personal Area Network
PC	Personal Computer

PGP	Pretty Good Privacy
PIN	Person Identification Number)
POP	Post Office Protocol
PSTN	Public Switched Telephone Network
PMU	Project Monitoring Unit of SEMP, MoEF
PoPs	Points of Presence
PDB.	Power Development Board
PGCB	Power Grid Company of Bangladesh
PKI	Public Key Infrastructure
R	
RAM	Random Access Memory
RAS	Remote Access Server
RATs	Remote Administration Trojans (RATs)
RCC	Rajshahi City Corporation
RIBEC	Reforms in the Budgeting and Expenditure Control
REB	Rural Electrification Board
S	
SMTP	Mail Transfer Protocol
SCADA	Supervisory Control and Data Acquisition
STP	Software Technology Parks
SME	Small and Medium sized Enterprise (company)
SDNP	Sustainable Development Networking Programme
SEMP	Sustainable Environment Management Program
SWMC	Surface Water Modeling Center
SMW4	SEA-ME-WE-4
SW	Short Wave
SPARRSO	Space Research and Remote Sensing Organization
T	
TRIPs	Intellectual Property Rights
TCP	Transmission Control Protocol

TDMA	Time Division Multiplexing Access
U	
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
USA	United States of America
UETA	Uniform Electronic Transactions Act
UCC	The Uniform Commercial Code
UGC	University Grants Commission
US	Unnayan Shamunnay
UPS	Uninterruptible Power Supply
UHF	Ultra High Frequency
V	
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal
VSAT	Very Small Aperture Terminal
vISP	Virtual ISP
VHF	Very High Frequency
W	
WAN	Wide Area Networks
www	World Wide Web
WPAN	Wireless personal area network
WAP	Wireless Application Protocol
WAN	Wide Area Network
WDMA	Wavelength Division Multiplexing Access
WISP	Wireless Internet Service Providers
WLL	Wireless Local Loop

BIBLIOGRAPHY

A.

1. A Comprihansive Guid to Cyberlaw,
2. Androw S. Taneubaum;
   Computer Networks; 3rd. Ed. 2000;
   Prentice Hall of India Private Ltd.,New Delhi.
3. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne;
   Operating System Concept; 7th Ed.,
   John Wiley Sons Inc.

B.

4. Behrouz A. Forouzan;
   Data Communication & Networking; 4th Ed. 2007-2008;
   Tata McGraw-Hill Publication Co.Ltd. New Delhi, India.
5. Barlow,
   A Declaration of the Independence of Cyberspace
6. Bangladesh Computer Council,

E.

7. Evidence Act.

F.

8. Lawrence Lessig's Code 190
9. Larry L. Peterson and Bruce S. Devid;
   Computer Networks, A System Approach; 2nd. Ed.;
   Morgan Kaufmann Publishers Inc., USA.
   First Print in India, 2000.

I.

10. Peter Norton;
    Interntroduction to Computers, Sixth Ed. 2006-2007;
    Tata McGrow-Hill Publishing Co. Ltd, New Dehi.

J

11. Jhons Wallace;
    Bill Gates and the Race to Control Cyberspace Overdrive;
    Jhon Wiley & Sons Inc.

L

12. Larry L. Peterson & Bruce S. Davia,
    Computer Net works;
    Morgan Kaufmann, 2nd Ed.

M.

13. Michael L. Carroll ;
Cyberstrategies;
Van Nostrand Rein Hold, New York.

N.

14. Nancy A. Lynch;
Distributed Algorithums
Morgan Kaufmann Publishers Inc., USA.
First Print in India, 2003.

P.

15. Penal Code,

T.

16. The code of Criminal procedure1898.
17. The computer Jagat, a monthly Magazine
18. The Internet Service Providers Association,
19. The (Indian) Information Technology Act. 2000,
20. The Constitution of People Republic of Bangladesh,
21. The Fourth Amendment to the United States Constitution
22. Thiru Thngarathinan;
Professional ASP Net 2.0 XML; Ed. 2006;
Wiley PublicationInc.

S.

23. Seymour Lipschutz, MarcLars Lipson;
Scheum's Outlines, Discreate Mathematics;
Tata McGrow-Hill Publishing Co. Ltd, New Dehfi.

W.

24. Wikipedia a free encyclopedia,
25. William Stalling;
Computer Nerworking with Internet Protocols & Technology;
Published by Dorling Kindersly (India) Pvt. Ltd.
26. William Lawton, Bradley Noe, Marcelo Lopez;
Development Multimedia Applications under OS/2;
John Willy & Sons, Inc, New York.

—The End—