Chapter II

Conceptual Notions of Cyber Crime
CHAPTER II
CONCEPTUAL NOTIONS OF CYBER CRIME

A. Introduction

A law is a body of rules laid down for determining legal rights and legal obligations which are recognized by courts.\(^1\) It is a command enjoining a course of action. The command emanates from sovereign or political superiors and is addressed to political inferiors. It may be the command of a legally constituted body or a legislation flowing from a duly constituted legislature to all the members of society. Law, according to Bodenheimer, is thus a synthesis of order and justice; they are locked together in a higher union.\(^2\) In the words of Professor Holland a law is “a general rule of external human action enforced by a political sovereign authority.”\(^3\) Law in its ideal is the statement of a principle of right in mandatory form by competent authority with adequate penalty for disobedience.\(^4\) It is rather a guideline for conduct and the art of what is right and equitable\(^5\). A crime is, therefore, an act of disobedience to such a law. However, disobedience of all law may not be a crime. For example, disobedience of civil laws (e.g. law of contract, law of inheritance) is not a crime. It is something more than a mere disobedience to a law.\(^6\)

Crime is a legal wrong which may culminate into punishment. It is a legal concept having the sanction of the law. Crime as a social and economic phenomenon found in the oldest human society. The Quran and Bible quote the murder of one son by another son of Adam. This was the

---

6. Ibid. p.4.
oldest crime. Crime entails punishment. Every crime has one standard of judging it, i.e., whether the act or omission is being followed by penal consequences. If it is not followed by punishment it may be a social wrong but not crime. A crime is conduct which includes action and omission both.

The expression Crime is defined as “an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The term ‘offence ‘is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force.” It is a social and economical phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.” The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin “the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences”.

According to Stephen “a crime is an act which is both forbidden by law and revolting to the moral sentiments of society.” But this definition is too wide to be accepted as the precise definition of the term crime since disobedience of civil, revenue laws or laws of contract are not crimes. Moreover, the moral sentiments and values of a society or a country are flexible, changing from time to time and place to place. For example ‘hearsay’ was once a crime in many countries, but it is not so now because it does not offend the moral sentiments of the society. Similarly sodomy (buggery) and adultery are crimes under the

---

7 Cyber Crime Scenario in India (B. Muthukumaran), criminal investigation Department Review-january 2008
8 Ashish Pandey, Cyber Crime Prevention and Detention Ist Ed.2006 p -1
Indian Penal Code, but it is not so in some western countries. Committing ‘Sati’ was not a crime in India until it was declared by legislation. Polygamy was allowed in India up to 1955 and it was not a crime but by the Hindu Marriage Act, 1955, it is made a crime. Thus, what was a virtue yesterday may become a crime tomorrow and vice versa. Consequently the content of a crime is volatile and fluctuating from time to time in the same country at the same time. Russell, therefore, rightly observed that “the task of defining crime has not been satisfactory accomplished by any writer.”

Crime have been described to be social injuries by Taft, who further maintains that the crimes vary according to the social values of the times and as such are subjective concepts. They have observed that ‘crime is but one form of social injury. Injuries are defined in terms of the values cherished in any society: in nearly all societies life and property are valued; to steal and to kill are, therefore, rated as injuries. Being thus defined by group opinions injuries are subjective concepts. They vary at different period in any changing society, and they vary between societies. Injuries are thus relative as well as subjective concepts’. This description of crimes may meet the requirements of a sociologist but not that of a legalist.

The essential of the command of political superior and the penalty are lacking in this description. The concept of law as a command of a political superior with power to enforce it is more pronounced in the context of criminal law and crimes, insofar as nothing is an offence which has not been so declared and laid down by law. Social injuries may be

10. Sec. 377, IPC
12. The Hindu Marriage Act, 1955 does not apply to Mohammedanas and Christians.
13 Russell: On Crime, vol. 1 (Edn. 11), p-18
termed as in the context of religious texts or immoral conduct in the eyes of moralists, but neither a sin, nor immoral conduct, nor anti-social behavior, can be termed a crime until it has been so declared by law. Thus, a social injury may be sinful, immoral or contrary to public good but not essentially a crime. According to Sutherland, ‘a combination of two abstract criteria is generally regarded by legal scholars as necessary to define crime, namely: legal description of an act as socially injurious, and legal provision of penalty for the act,’ and both these requirements are the product of positive law. It would not be inappropriate to say that crimes are merely ‘acts forbidden by the law under pain of punishment.’

In the eye of the law a crime is a wrongful act or omission which has been made punishable in criminal proceedings as a matter of public policy by law and is intended to secure peace, security and harmony by protecting the person and property of the members of the community.¹⁴

Crime may not be purely a legal problem, rather may as much be a social and economic problem in view of its consequences and therefore is considered to be a wrong against the State and society; nonetheless the essential elements of a crime are that it is conduct forbidden by law laid down by the State and is made punishable by the law Nulla poena sine lege has now come to be accepted as the most important element of criminal law. It implies that no person may be punished except in pursuance of a statute which prescribes a penalty and therefore strictly speaking no conduct may be held criminal unless it is precisely declared so by criminal law. Crime is what criminal law has so declared.

The Concept of Crime

The concept of crime is essentially concerned with the conduct of individual is society. It is well-known that the man by nature is social and his interests are best protected as member every one owes certain duties towards his follow-men and at the same time has certain rights and privilege which he expects other to endure for him. It is this sense of respect and trust for the rights of others and duty consciousness of the member of the society which regulates their conducts inter se. Although most people prefer to follow a “Live and Let-Live” policy, there are few who for some reason or the other deviate the normal path and associate themselves with anti-social activities.

This obviously imposed an obligation on the State to maintain normalcy in society. This arduous task of determining as to what is rightful or wrongful conduct is performed through the instrumentality of law which according to Salmond is “Rule of action’ regulating the conduct of individuals in society. The conducts which are prohibited under the existing law at a particular place are known as wrongful acts or crimes, while those which are permitted under the law are treated as lawful. The wrongdoers committing crimes are punished for their guilt under the law of the land.15

Early concept of Crime:

Crime has been a baffling problem, ever since the dawn of human civilization. Crime is a constant phenomenon changing with the social change. Historically, the concept of crime seems to have always been changing with the variations in social conditions during the evolutionary stages of human society. Early English society during 12th and 13th

---

15 K.D.Gaur: Criminal Law and Criminology, p-30, 2002
centauries included only those acts as crimes, which were committed against the state or the religion. Early societies recognized no distinction between the law of crimes and torts but only knew law of wrongs. The English society prior to 10th centaury confused crimes with torts because the bond of family was far stronger than that of the community, the injured party and his kindred could avenge the wrong by private vengeance and self-redress and recourse to legal remedy was considered merely an optional alternative to self-redress. The wrongdoer was supposed to offer compensation to the person wronged, the quantum of which dependent on the extent of the wrong caused and the status of the sufferer. It can therefore be observed that the law did not play compelling part in regulating the social relations in early days as it does today. The modern legal systems provide that as soon as an offence is committed, the law is set into motion at once irrespective of the wishes of the injured party, whereas in early societies the law was administered only if both the parties agreed to submit themselves to the verdict.  

The period of 18th centaury witnessed an era of miraculous reorientation in criminology. The Idea that crime was the result of divine displeasure, the superstitions and myths were all abandoned and the study of crime and criminal was started afresh on a scientific basis and firmly believe that no one else than the offender himself could be attributed criminal responsibility for his crime and the external agencies had nothing to do with it. And hence, it would appear that the concept of crime is closely related to social policy of a given time. The concept of crime also changes, with changes in ideologies. After that, certain new crimes spring up whereas some existing crimes become obsolete and therefore, they are deleted through adequate changes in the criminal law.

The criminal law has often been considered as a barometer to gauge the moral turpitude of the society at a given time. In other words, the social standards of the society can conveniently be judged by studying the criminal policy adopted by it.

There has been considerable increase in crime rate in recent decades. The incidence of crime in western countries is far greater than that of India perhaps, because of the variance of social conditions in these countries. The factors such as the greater control of family over the wards and respect for morality and religion, etc. have acted as effective restraints to reduce the incidence of crime in India. The upward trend in crime-rate can be attributed to modernization, urbanization, industrialization, advance of science and technology and growth of civilization, and advent of materialism and now the internet. Scientific know-how has proved a boon to criminals in carrying out their criminal activities with considerable ease, which provides better opportunities for escape and avoid detection. The risk, involved in committing crimes is also lesser. This calls for greater need for a new approach to crime and criminals so as to cope up with the new situations and keep crimes well within control.17

The law is variant in character, so forever changing, adding new crimes to the catalogues and modifying, altering and repealing former ones. There have been astonishing changes in the area of the crime. Technological innovations in crime, terrorism and economic coercion are the major hazards posing challenges all around the world. Today crime has been computerized and financially sophisticated.

Definitions of Crime:

Sir William Blackstone in his classical work, *Commentaries on the laws of England, Volume IV*, which is devoted to, “Public Wrongs or Crimes,” attempted to define crime at two different places in his work. At one place, he states that crime is:

*An act committed or omitted in violation of a public law forbidding or commanding it.*

At second place, he states that crime is:

*“a violation of the public rights and duties due to the whole community considered as a community.”*

This definition has been slightly altered by the learned editor of Blackstone, Serjeant Stephen, who expresses it thus:

*A crime is a violation of right, consideration reference to the evil tendency of such violation as regards the community at large.*

*Austin* has, in defining crime, observed:

*A wrong which is pursued at the discretion of the injured party and his representatives, is a civil injury; a wrong which is pursued by the sovereign of his subordinates is a crime.*

*Professor Kenny* modifies Austin and defines crime to be “wrongs whose sanction is punitive and is in no way remissible by any private person, but is remissible bye the Crown alone, if remissible at all.

---

19. Ibid.
20. Stephen in Blackstone’s Commentaries, 5
21. Austin Jurisprudence, Lecture XXVII
22. Kenny: Outlines of Criminal Law
Professor Paton observes:

In crime we find that the normal marks are that the state has power to control the procedure, to remit the penalty or to inflict the punishment.

Similarly Professor Keeton says:

A crime today would seem to be any undesirable act which the state finds it most convenient to correct by the institution of proceedings for the infliction of a penalty, instead of leaving the remedy to the discretion of some injured person.23

Encyclopedic Dictionary

“A crime is an unlawful act or default which is an offence against the public and renders the person guilty of the act or default liable to legal punishment. While a crime is often also an injury to a private person, who has a remedy in a civil action, it is an act or default contrary to the order, peace and well-being of society that a crime is punishable by the state.24

Glanville Williams:

A crime (or offence) is a legal wrong that can be followed by criminal proceedings which may result in punishment.25

Miller: “A crime is the commission or omission of an act which the law forbids or commands under pain of a punishment to be imposed by the state by a proceeding in its own name.26

23. R.C.Nigam, Indian Penal Code, Vol. 1, p. 470
26. Miller: Criminal Law, p. 15
Looking to the above definitions it become clear that a crime is a harm brought about by human conduct which the sovereign power in the state desires to prohibit. Among the measures of prevention selected is the threat of punishment and legal proceedings of a special kind which are employed to decide whether the person accused did in fact cause the harm, and is according to law to be held legally punishable for doing so.

**Information Technology**

We are living in an era of internet and information technology. The information and communication technologies have been revolutionized in the past two decades. The invention of the computer has been a boon to the human community. The 21st century known for knowledge driven society and man has always been motivated by the need to better the existing technologies and this has led significant development and progress. The information and communication technologies revolutionized with the invention of computer and computer has been a boon to the human community, but the same computer is an instrument to aid criminals.  

Computer revolution has given birth to internet culture. Internet is a massive worldwide network of computer connected to each other with the main objective of sharing and transmitting information. The internet is a global network in interconnected computers, enabling users to share information. Typically, a computer that connects to the Internet can access from available servers. A majority of widely accessible information on the Internet consists of inter linked hypertext documents and other resources of the World Wide Web (WWW).

---

27 Nuzhat Parveen Khan, “Cyber Crimes and the Adequacy of the EXXI 2004, The Bar Council of India trust, New delhi, p-121
The internet is still at a vary nascent stage of development. Being the newest mode of communication, the laws railing them are also at a developing stage. As the internet gain proliferation, so will the complexity of Cyber Laws covering more relevant more relevant issues. With many countries and societies are in the process putting in place the Cyber Laws, a few have already put down Cyber Laws and India is proud to be one among them. India is globalizing its economy.

Information Technology and Information Services have a profound effect on the country’s economy, trade and commerce. The Securities and Exchange Board of India has allowed trading on the Internet. The Stock Exchange in India is carrying out different kinds of transaction and information exchange of their networks. The Reserve Bank of India has introduced the electronic payment system. There have been concerns from Intelligence and Law Enforcement Agencies and other about Computer Crime, Computer misuse, data protection, security standards, intellectual property rights, privacy etc.  

The movement of information in the Internet is achieved via a system of interconnected computer networks that share data by packet switching using the standardized Internet Protocol (TCP/IP). It is a “network of networks” that consists of millions of networks and is linked with wireless connections and other technologies.  

Anything related to Internet and computer networks came to be known with the prefix ‘Cyber’-Cyber law, cyber café, cyber police, cyber space, cyber stalking and cyber fraud. The list is endless. Internet

28 V.D. Dudeja: Crimes in Cyber space Scams & Frauds (issues and remedies), Edn. Ist 2003, pp-221-222
29. Transmission Control Protocol/Internet Protocol – The TCP component is responsible for converting message into streams of packets whilst the IP is responsible for addressing and routing the packet to their intended destination.
provides as superhighway for transportation of information. It is popularly known as “World Wide Web” (WWW). The Internet is fast becoming a way of life for millions of people.\(^{31}\)

**Internet and Cyber Crime**

At the outset it would be pertinent to mention that Internet is the only mode and medium for commission of cyber crime, therefore, it becomes necessary to deal with the Internet, various modes of access to Internet and different modalities of communication through Internet. In fact the importance and dependence of the modern life on computers and Internet cannot be ignored since it has become indispensable almost in all walks of life and human transactions, such as hospitals, educational institutions, industries, railways, aviation, shipping, space science, nuclear energy etc. Computers get associated with a person before his birth when CAT scanners detect birth defect or determine sex and remain associated for sometime even after the death till insurance issues are settled.\(^{32}\) Computers have invaded every aspect of the life and the impact has been so quick that it caught the institutions of law and justice unawares. The new developments are posing challenges to the fundamental principles of law, which worked well before the advent of this technology. The problems have been compounded by the introduction of Internet.

In India, most of the laws are either of British origin or passed after the first three decades of Independence. During this period computers had not made so much influence as we see today and Internet, during this period, simply did not exist. Most of the existing laws assume physical environment, geographical boundaries, tangible documents and records.


As against this, in a digital world everything is recorded in digits, without any respect for political boundaries and can be modified, altered and replaced without any murmur.

Law cannot afford to remain oblivious of these developments and lose relevance. That will be simply to delay inevitable. Law has to cope up with these new challenges and in the changing scenario, redefine the roles of individuals and groups, the relationship between the entities and inter se rights and obligations. The situation demands that there should be a concerted effort on the part of the lawyers, judges and legislators to resolve the legal issues raised by the introduction of information technology. There is a genuine feeling that the new world of digits demands training not only to the Bench and the Bar but also to law enforcement agencies as new language has been introduced which has given new meaning to old words.

**Communication through Internet**

For the proper understanding of legal issues involved in Internet communications, a basic understanding of access to Internet, and modes of communication available to transfer information through Internet is *sine qua non*.

Generally, three methods are available for a user to access to Internet. These are: -

a. Direct access
b. Internet service providers
c. Commercial online Service
a. **Direct access**

As the expression itself suggests, a user can be directly linked to Internet without any intermediary. Generally, government offices, educational institutions, research centres, libraries and even business establishments, corporations and companies maintain a computer network linked directly. These establishments then issue an account number with a secret key called “password”. The account number together with the “password” enables a user to have an access directly to Internet. This direct access is not economically viable.

b. **Internet service providers**

Service providers are generally commercial entities making commercial use of Internet by making available Internet information to general public in lieu of the fee that the user has to pay. Service providers have direct access to internet and any “PC” holder can have access to Internet only via direct link holder. It works just like a home telephone without STD facility. However, there is a difference between the two. In case of telephone only one time access is possible if subscriber wants to have STD facility, he can get that directly and permanently also. The service provider offers access to Internet generally on monthly basis by charging fee.

c. **Commercial online service**

Commercial online service provides direct access to users without any fee. However, the commercial online service provides extensive content of the information within their proprietary networks. These services are at present provided by online services such as American online, CompuServe, Prodigy and the Microsoft Network.
These are commercial entities and provide their own content to the user of their service.

**Modes of Communication**

The exchange of communication and retrieving of information on Internet is possible through many modes. However, these modes are constantly changing so an exhaustive list cannot be expected. The popular methods of communication are grouped as follows:

a. One to one communication (such as “e-mail”)

b. One to many communication (such as listserv”)

c. Sharing of information databases (such as ‘USENET newsgroups”)

d. Real time communication (such as Internet Relay Chat)

e. Real time remote computer utilization (such as “telnet”)

f. Remote information retrieval (such as “ftp”, “gopher and the “world wide web”)

   a. **e-mail**

A user having system linked with Internet can communicate information through electronic mail more popularly called “e-mail”. The communication through e-mail is possible to one or more other users. As Internet does not have central controlling or storage point, so “e-mail” can take many and different paths to recipients. The electronic mail can be compared with an ordinary letter. However, it has many limitations. For instance, the message sent remains open and can be accessed or viewed on any intermediate computers between the originator\textsuperscript{33} and

\textsuperscript{33} Originator is a person who sends, generates, stores or transmits any electronic message or causes any electronic messages to be sent or transmitted to any other person but does not include any intermediary. See Section 2(z) of the Information Technology Act, 2000.
addressee\textsuperscript{34} unless the message is encrypted. The registered mail, as we understand in ordinary postal system, does not exist in Cyberspace. So “e-mail”, at present, cannot be sealed and is, therefore, not a secured one.

Another serious disadvantage is that the originator does not know whether the addressee has received the mail or not and there is, at present, no way to confirm it.

b. **List Serv**

Listserv enables a user to establish a mailing list available on the Internet that carries topics of different interests. The user can choose any topic of his interest in the mailing list and subscribe it. He then receives a copy of messages posted by other subscribers and in turn can post messages for full mailing list. Once a mailing list is maintained, it is run with the help of “mail exploder”. The “mail exploder” is a software program, which run on the server that carries the mailing list. It responds automatically (without any intervention of a human being) to a user’s request to be added to or removed from the list of subscribers. It also carries messages posted by a subscriber to others on the mailing list. All messages posted by a subscriber to others on the mailing list are forwarded to a “moderator” who selects the message for retransmission. The mailing list may be “closed” or “open”. In “closed type”, mailing list cannot be established unless there is a previous approval for joining the list. In “open type”, a user can join the list without any approval. However, in both these situations, retransmission of message is subject to the approval of the moderator.

\textsuperscript{34} Addressee is a person who is intended by the originator to receive the electronic record but does not include any intermediary. See Section 2(b) of the Information Technology Act, 2000.
c. **Sharing of Information Databases**

This method of communication has made real beginning in the sharing of knowledge. Knowledge has no longer remained a reserved source but a common pool to be shared with all and sundry. Write ups can be transmitted or received through Internet, which are daily posted to thousands of discussion groups known as “newsgroups”. These write-ups are arranged according to subject-matter and are available through an electronic Bulletin Board known as “Usenet”. In “newsgroups” innumerable persons can participate in discussion and users can access the database at any time without subscribing to the discussion mailing list in advance as is the case with listserv.

d. **Real Time Text Based Communications (Talk and IRC)**

This mode of communication has virtually relegated Internet to ordinary telephone. By using program “talk”, two users online can interact with each other. The words written on one computer will immediately appear on the screen of other. The program of “chat” such as “Internet Relay Chat” (IRC) allows different users to converse by selecting one of many discussion channels active on any time. These channels make possible for a user to see, read and talk to other user without seeing his face. Here users may adopt pseudo names with impunity.

e. **Real-Time Remote Computer Utilization (Telnet)**

Telnet is one of the applications of Internet, which makes possible for a user to make his personal computer as terminal to a remote system. It can help a researcher to use computing power of Super Computer located at different places.
f. **Remote Retrieval of Information**

Access to and retrieval of information, located at any computer, having link with Internet, has become most popular function of Internet. This is possible by three methods, which are “ftp”, “groper” and “www”. In “ftp”, the files available on the remote computer are listed and copies of the files required are transferred to individuals. “Groper” acts as a search guide and helps an individual to locate desired information from available resources on a remote computer.

The most popular and latest method of search and retrieval of information on remote computer is World Wide Web (www). It uses “hypertext” formatting language commonly called HTML (hypertext mark-up language). A viewer of the document can connect the links provided by HTML document by a click of “mouse”, to other related information or other resources on the Internet. “Hypertext” links help a user to reach an information stored in a computer situated in any part of the globe. Users can reach directly also to source by taping an Internet address of the document in the Uniform Resource Locator (URL).

Publication of information on web is an issue, which concerns while legal fraternity, be it constitutional experts, businesses or criminal law lawyers. An information is said to have been published when it is made available on the “world wide web” which is possible only when the user interested in the publication of the information connects his computer to Internet by running information is free to make his information available to all Internet users or to limit it a particular class who can have access only after prior permission. Generally, publishers are interested in wide publicity so they keep their sites open to all users. However, a site can be made a “closed one” by assigning specific names and ‘passwords’ as a precondition to access the site.

---

35 “ftp” stands for file transfer protocol.
Cyber Crime

The use of computer in law is of recent origin. As late as 1979 Fielder in his work “Functional Relation between Legal Regulation and Software” lamented that “on the side of the legal theory up till now there has been but very little interest in the computerized implementation of law. For legal theory, this lack of interest is a deplorable deficiency. “Now lamentable stage is over. Computer is used and is helping law experts in knowledge acquisition, knowledge representation and knowledge utilization. It is rightly said that technological development in every area is likely to cause drastic effect in every walk of life. It is evident that at present whole world is crazy for spaceman ship involving various adventures and causing revolutionary changes. The scientific and technological advancement specifically in the fields of communication and information have created havoc thus, opening new ventures for the human being including the criminals. On the other hand criminal minded people misused the said revolution for the promotion and extension of criminal activities. These activities may be referred as computer crime or cyber crime. Cyber crime is the most recent type of crime which affects many people. This is the biggest challenge for police, prosecutors and lawmakers.

Cyber Crime is a problem which confronts the entire world. Cyber Crime is the most dangerous of all crimes because of the magnitude of the loss it is causing today and its potential, the ease with which it is committed, its invisibility and the disregard for geographical boundaries, the difficulty in investigation, collection of evidence and successful prosecution of the cyber criminals and the costs of dealing with Cyber Crime by effecting law enforcement and protective technology. The Internet being an integral part of daily life, cyber Crime, if not checked
would be destructive to civilization itself. The growth of Internet linked with the growth of protective technology and other means to check cyber crime. It would be futile for Internet culture to grow without effective means of checking cyber crime. It would be in the interest of the society for the Internet, e-commerce e-business to grow slowly but steadily.\(^\text{36}\)

The term ‘cyber crime’ is a misnomer. This term has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. Cyber crime has not been defined in Indian Penal Code, 1860 because it was drafted in 1860 when computers were non-existent. Information Technology Act, 2000 is the only Act which gives legal recognition to computers and matters related thereto. The Information Technology Act, 2000 has for the first time brought cyber crime, punishment and procedure for probing it within a legal framework.

Cyber crime is an amalgamation of two words: ‘cyber’-related to internet or other electronic networks and ‘crime’-a criminal activity.\(^\text{37}\) Literally, the word cyber means “connected with electronic communication networks, especially the internet\(^\text{38}\).”

“Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime”.

“Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime”.

\(^{36}\) V.D. Dudeja: Crimes in Cyber space Scams & Frauds (issues and remedies), Edn. Ist 2003, p-220
\(^{38}\) According to Oxford Learners Dictionary.
A generalized definition of cyber crime may be “unlawful acts wherein computer is either a tool\textsuperscript{39} or target\textsuperscript{40} or both”. The term “computer” used is in this definition does not only mean the conventional desktop to laptop computer. It includes Personal Digital Assistance (PDA), cell phones, sophisticated watches, cars and a host of gadgets.

Cyber crime is the use of computers and the internet by criminals to perpetrate fraud and other crimes against companies and consumers. Crime committed using a computer and the internet to steal a person’s identity or sell contraband or stalk victims or disrupt operations with malevolent programs. Cyber crime is a broadly used term to describe criminal activity committed on computers or the Internet. Some of it is punishable by the laws of various countries, where others have a debatable legal status.

Cyber crime has been defined as the act of creating, disturbing, altering, stealing, misusing and destroying information through the computer manipulation of cyberspace; without the use of physical force and against the will or the interests of the victim. As a concept, information can be anything from electronic money, to government secrets, and the victim can be an individual, a corporate person, or as criminal law is defined: the state and society as a whole.\textsuperscript{41}

However, the term cyber crime is also used to denote all those objectionable activities, misuse or abuse that they are either conducted in

\textsuperscript{39} Cybercrimes which involves computer as a tool are usually modification of conventional such as drug trafficking, on-line gambling, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyber stalking, spoofing etc.

\textsuperscript{40} Cybercrimes where computer is a target include sophistical illegal activities such as unauthorized access to networks or computer systems, e-mail bombing, Trojan attacks, data diddling, denial service attack, Internet time theft, logic bombs, virus or worms attacks.

\textsuperscript{41} Cybercrime: A Challenge to Leviathan, \url{http://www.lse.ac.uk/club/hayek/Essays/cybercrime.htm} visited at 04/03/2010 at 1:15 PM.
the cyber world, or through or against a computer. It is an umbrella term and may have different meaning in different situations.42

The first recorded cyber crime took place in the years 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 BC in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.43

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of series of steps in the weaving of special fabrics. This resulted in a fact amongst Jacquard’s employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from use of the new technology. This is the first recorded cyber crime.

Today, computers have come a long way with neural network and nano-computing, promising to turn every atom in a glass of water into a computer capable of performing a billion operations per second.

In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications. Cyber Crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief. The abuse of computer has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc.44

Prof. S.T. Viswanathan has given three possible definitions of cyber crimes and these are as follows:

(a) Any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer.

(b) Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

(c) Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmitting of data.\(^{45}\)

Douglas Thomas and Brian D. Loader\(^{46}\) has attempted the definition of cyber crime in its broadest contours by observing that “cyber crime can be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by the new Information & communication technologies ICTs. The global connectivity of the Internet, for example, makes it much easier for criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing organized crimes to use more sophisticated techniques to support and develop networks for drugs trafficking money laundering, illegal arms trafficking, smuggling and the like. For hackers with the requisite computer skills, a large market exists for security and trade secrets which can be accessed transmitted electronically. Furthermore, the many-to-

\(^{46}\) Douglas Thomas and Brian D. Loader, Cybercrime: law enforcement, security and surveillance in the information age at p. 3
many communications which is an essential feature of the Internet enables the production and worldwide dissemination of information and knowledge which could be potentially harmful, threatening or liable to incite violence.

Of even greater significance perhaps is the blurring of the distinction between internal and external security. The transforming qualities of ICTs make it increasingly difficult to distinguish between warfare, terrorism and criminal activities. Extremist political groups, for example, may engage in all the three. A country in the post Cold War period may be more under threat from economic espionage than nuclear assault. The use of ICTs by non-government organization and international criminal organizations will therefore clearly have a increasingly important impact upon the functioning of law enforcement and security agencies in the information age.  

**United Nation’s Definition of Cyber crime**

Cyber crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standards definition of the crime. At the Tenth United Nation Congress on the Prevention of Crime and Treatments of Offenders, in a workshop devoted to the issue of crimes related to computer networks, cyber crime was broken into two categories and defined thus:

(a) Cyber crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them,

49. Tenth U.N. Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.
(b) Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definition are complicated by the fact an act may be illegal in one nation but not in another. There are more concrete examples, including

(i) Unauthorized access
(ii) Damage to computer data or programs
(iii) Computer sabotage
(iv) Unauthorized interception of communications
(v) Computer espionage

These definitions, although not completely definitive yet it gives us a point to begin with where there has been a global recognition and agreement for discerning the whole gamut and amplitude of cyber crime and what it actually connote that may usher the world community to take concrete and resolute efforts collectively to combat the challenges posed by it.

The present scenario of Cyber crimes is summed up in the following words:

Amidst the surging excitement and interest, however, runs a deep thread of ambivalence towards connecting to the Internet. The Internet’s evil twin is the home of “Bad Guys”-hackers, crackers, snackers, stalker,
The unprecedented growth of computers and the Internet is revolutionizing almost all aspects of human life. Increasing use of computers and the Internet in government, military institutions, critical services like power, telecommunication and aviation, education, financial sector and banking is undoubtedly moving the present day society into a new information age parallel only to the Industrial Revolution. Among developed nations, computer has become an item of necessity in every household. India is also catching up with other countries, standing fourth among the top then nations in the world with 81 million internet users. The growth of mobile phone in India has also been phenomenal. In addition to being a communication device, the mobile phone offers connectivity with the Internet. Many new applications, like Twitter’s Tweet SMS are also available on cell phone. The global sweep of the Internet, providing a borderless and a relatively anonymous domain has brought many opportunities for activities that are undoubtedly of criminal nature. The Internet has made it possible to commit computer crime from

50. Farooq Ahmad, Cyber Law in India, Edn. IIIrd, 2008, p-367
51. These statistics were released by the Internet Governance Forum on the eve if is 3rd four-day global conference held at the Hyderabad International Convention Centre, Hyderabad on December 3-6, 2008. [http://economictimes.indiatimes.com/Infotech/India_ranks_fourth_in_world_with_81_million_interne t_users/articleshow/378138.cms]
52. According to Telecom Regulatory Authority of India mobile operators a record 15.64 million customers in March 2009. The Mobile subscriber base in India rose by 50% or more than 130 million to 391.8 million. (Fact recorded on: April 22, 2009; [http://www.itfacts.biz/3918-min-mobile-subscribers-in-march-2009/12961]
53. An Internet browser firm Opera, in its latest report out a strong signal to the mobile Internet industry – in July nearly 29.1 million people worldwide used Opera Mini which is most widely downloaded mobile app. According to the report India continued to move up the top 10 list of countries, overtaking China for 3rd place. [http://trak.in/tags/business/2009/08/26/mobile-internet-usage-india/; http://www.livemint.com/2009/04/27123552/Mobile-web-usage-rose-193-in.htm]
54. India recently became the 3rd largest online market for Twitter in just a few months, with 5 million subscribers of a total of over 11.5 million. Airtel, largest cell phone, service provider has an exclusive arrangement with Twitter to offer the service. [http://telecomtalk.info/airtel-launches-tweetsms/11132]
a far off place, often beyond national boundaries. Three factors contribute to the increase in cyber criminality. They are:

(a) Volume of e-commerce and online corporate transactions

(b) Better and faster connectivity both for target of crime and offenders

(c) Increased vulnerability of targets

The unbounded cyberspace has offered, both to the novice and organised criminals, avenues for committing cybercrime. The ability and ease with which cyber criminals may place automated software to collect information from computers connected to the Internet has been a major concern of individuals, business organizations and Governments.

**Distinction between Conventional and cyber crime**

There is apparently no distinction between conventional and cyber crime. However, on a deep introspection we may say that there exists a fine limit of demarcation between the conventional and cyber crime, which is appreciable. The demarcation lies in the involvement of medium in cases of cyber crime. The *sine qua non* for cyber crime is that there should be an involvement, at any stage, of the virtual cyber medium.\(^{55}\)

Cyber crimes can be defined as any crime with the help of the computer and information technology with the purpose of influencing the functioning of computer or computer system.\(^{56}\) This term could reasonably include wide variety of criminal offences and unlawful

\(^{55}\) Ashish Pandey: Cyber crimes Detention and prevention, 2006, p- 1.2

activities related to or having connection to computers or a traditional crime which has been transformed by the use of a computer.

Cyber crime is the latest and perhaps the most complicated problems in the present world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime. Therefore, Crime is a legal concept, it has social and economical phenomenon which is as old as human society. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.”

Cyber crimes are different from conventional crime, as they can be easily committed from distant place, difficult to detect and even harder to prove them. It is very difficult to identify the culprit, as the net can be accessed from any part of the globe. The cyberspace is wide open for the cyber criminals for criminal activities.\(^\text{57}\)

Cyber crime is an offence just like any other offence. Cyber crime or conventional crime both includes conduct of act or omission, which is prohibited by law of state and is punishable. Cyber crime is a crime in which computer is used for an act or omission for committing offence. In committing cyber crimes computer is used as instrumentality as a means of perpetuating further crimes. In cyber crimes computer may be a tool or target.\(^\text{58}\)

**Essential Elements of Crime**

It is general principle of criminal law that a person may not be convicted of a crime unless the prosecution has proved beyond reasonable doubt that:

\(^{58}\) Dudeja V.D.: Cyber Crime Law Enforcement (Commonwealth Pub. Delhi) 2003, P.82
(a) He has committed a criminal act, or incurred a responsibility to be attributed to him for the existence of a certain state of affairs, which is forbidden by criminal law; and

(b) He had a defined state of mind in relation to the causing of the event or the existence of the state of affairs.

Thus, a crime essentially consists of two elements, namely actus reus and mens rea.

So for existing criminal liability there must be actus reus and mens rea i.e. wrongful act and wrongful intention. Wrongful act in itself is not sufficient for punishment because there is a legal maxim viz. actus non facit reum nisi mens sit rea i.e. act only does not constitute a crime unless the act is done with guilty intention.

**Actus Reus**

The actus reus, then, is made up generally, but not always, of conduct, and sometimes its consequences also the circumstances in which the conduct takes place, or which constitutes the state of affair, in so far as they are relevant. Sometimes a particular state of mind on part of victim is required by the definition of the crime. If so, that state of mind is part of the actus reus.

**Actus Reus in Internet Crimes**

In computer crimes the element of actus reus is easy to identify, but not so easy to prove. Some of the examples actus reus in computer crimes may be identified as:

i. Doing something which makes a computer function eg. Touching keyboard and mouse.
ii. Trying to access data stored on a computer or from a computer, which has access to data stored outside.

iii. Using internet to attempt to gain access, signal pass through various computers. Each of these computers is made to perform a function on the instruction which the person gave to the first computer in chain. Each activity constitutes *actus reus*.

**Mens Rea**

The second element of crime *mens rea* or guilty mind may comprise a number of different mental attitude including intention, recklessness and negligence etc.

**Mens Rea in Internet Crimes**

Regarding mens rea in internet crimes, C. Gringras\(^{59}\) observed that “in computer crimes an essential ingredient for determining mens rea on the part of offender is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized. There must, be on the part of the hacker, intention to secure access, though this intention can be directed at any computer and not at a particular computer. Thus, the hacker needs not be aware of which computer exactly he or she was attacking. Further, this intention to secure access need not be directed at any particular kind of programme or data. It is enough that the hacker intended to secure access to programmes or data *per se*.” Therefore, like traditional crimes *mens rea* is equally a pre-requisite to establish the guilt of the cyber criminal.

\(^{59}\) C. Gringras: The Laws of the Internet at p. 221
Thus, there are two vital ingredients for mens rea to be applied to a hacker:

(a) The access intended to be secured must have been unauthorised; and

(b) The hacker should have been aware of the same it the time he or she tried to secure the access.\(^6\)

**Evolution of Cyber Crime**

Prior to the turn of the millennium large scale cyber crimes were centered on or around one-man operated criminals exploiting the weaknesses in the computer operating system or computer network. In most cases these crimes were committed by computer nerds who felt challenged to prove that they could beat the system. We coined the term hacker for just such a nerd, but rarely was there a financial gain element to the criminal behavior.

While a great deal of financial damage could actually result, not to mention the potential for the security risks that resulted, this one-man band criminal lacked the motive and intent of traditional criminal gangs. In short, cyber crime was infantile and largely seen as a practical joke or game by those who committed it. Criminal defense tactics at this time was also largely based on the fact that no real intentional damage was done and, in a large number of cases, the penalty for the crime was showing how the computer system had been hacked by the hacker.

Once we had all got over the fact that there was no millennium bug after all (probably the biggest cyber crime hoax of all time), cyber criminal had organised and focused their attention elsewhere. Yes, the

geek element of hacking still existed – as still does today – but how hardened criminal gangs had worked out that the Internet was a safe domain, with much less risk, with which to operate and generate large profits.

In short, criminal gangs had introduced a professional element into the world of cybercrime. No longer were we looking at geeky exploitation of weaknesses in computer operating/networking systems, things had now developed to criminal gangs making use of computer networks to infiltrate and take advantage of the trust of other users of that computers network for huge financial gain.

**Modus Operandi of Cybercrimes:**

The Internet has changed the subject-matter of crime and more importantly its *modus operandi*. The entire criminal act consists of automated machines and the human hand is only at the starting or ending points. This makes the challenges formidable. The challenges posed before the criminal system is mainly due to the following reasons:

1. The transnational nature of cybercrimes where geographical limits and international boundaries have lost their meaning and a single criminal act passes through a number of jurisdictions.

2. The ever-expanding nature of the Internet and the backwardness of the present criminal law have rendered law, helpless and unresponsive.

3. The technicality involved in cybercrimes makes investigation a highly complicated and purely technical job.

---

4. Lack of visual evidence (LOVE) in detecting cybercrimes throws biggest challenges to the legal system which is mainly based on evidence of some sort.

Cybercrimes are crimes of the digital age. They are bloodless, non-violent types of crime which are committed by computer literate persons whose way and method of committing the crime is highly sophisticated and technical. Most of the cybercrimes are committed by a good number of accomplices called “outsiders and insiders” who are workers of communication and Internet service companies. *Modus operandi* is a system of actions of the criminal (and/or related persons) united by one intention directed on preparing, committing and covering up a crime, determined by objective or subjective factors and connected to use of corresponding facilities and means. *Modus operandi* of committing cybercrimes mainly involves illegal interference in computer, computer system and network operation. Such illegal interference can be divided into various groups through which the cybercriminals ensure their access to the targeted computer in which either data are stored or required information is preserved:

1. **Ways of Direct Access:**

   This covers damaging, deletion, deterioration, alteration, suppression or copying of computer data and includes unauthorised hindering of computer, computer system, or network functioning by inputting corresponding commands from the computer where information is restored. Such direct access can be made by both persons working with data and as well by persons intentionally penetrating in restricted areas or premises where information is restored. However, due to de-centralisation

---

of information processing, direct access is decreasing and the perpetrator finds it easier to intercept computer information during its transfer via telecommunication channels or computer networks. In order to seize information left by the user, the perpetrator looks around workplaces of programmers for drafts, and examines and restores erased software.\(^{63}\)

2. **Ways of Indirect Access:**

Ways of indirect access to information includes access without right to certain computer or information system via computer networks from the computer located at certain distance.

Following are the ways of indirect or remote access:

1. Connecting to telecommunication cable of authorized user (i.e. phone line) and obtaining access to his system. Penetrating in other information system by automated picking out of phone numbers of subscribers with further connection to their computers (picking out is carried out till the criminal receives the answer of the modem on the other side of the phone line). Often attempts of unauthorised access may be detected easily. This happens when similar hack is carried out from several work places: at a specified time, several PCs (more than 10) perform attempt of unauthorised access. System security may prevent several “attacks” and desirable illegal access. One of the penetrated computers blocks network “logging” system that fixes all access attempts. As a result, other penetrated computers may not be detected and allocated. Some of them start to hack a certain fake sub-network, other carry out fake operations in order to hinder functioning of the enterprise, institution, authority and cover up crime.

---

\(^{63}\) Ibid.
2. Penetrating in computer networks with the help of passwords, pretended to belonging to an authorised user is yet another mode to obtain access. By using this method, violators crack passwords with the purpose of access to other computers. There are several specially developed softwares for these purposes. They may be purchased from “shadow” computer market. Once the right password is obtained (it takes less than 24 hours for choosing eight-digit password), illegal user obtain access to computer information and may use it the way he likes, for instance, for copying, deleting, spoiling, modifying or suppressing computer data, perform operations like wire transfers, forgery of payment order, etc. as the authorised user.

Direct access includes methods of direct and electromagnetic interception of computer data. Direct interception is the simplest way of access without right. Interception is made through external communication channels or by way of direct connection to cables of peripherals devices. At that cable and wire system, land microwave systems, satellite communication systems and also government communication systems are the objects if direct listening.

Electromagnetic interception is done through latest technical devices which allow obtaining information directly without being connected to computer system. As a result of emissions, interception of central processors, display, communication channels, printers, etc. is possible. “Bugs” is one of the most popular electromagnetic interception. These “bugs” are sensitive microphones designed for listening to conversations of attendants.
3. Mixed methods:

These methods consist of both direct and indirect (remote) access. They are:

1. Secret insertion of commands in programs that allow the performance of new unplanned functions, making this program workable (program copies files, but simultaneously it deletes data on financial activity of an enterprise.

2. Alternations of programs by way of secret placing of command sets that should come into action under specified conditions and in a given time. Thus, as soon as the program illegally transfers money funds to so called false account, it will self-destruct and delete all the data on the committed operation.

3. Access is obtained to database and files of the authorised user through weak places in security systems. This gives an opportunity to read and examine information stored in the system and copy it. Thus, one may appeal to database of the competitor company and have an opportunity not only to analyse its financial state, but also to obtain evident advantages in competition struggle.

4. Mixed methods also include using of bugs in programs and files. The program is called “breaking” and malefactor inputs some amount of certain commands that help to perform new unplanned functions making this program runnable. Thus, one may transfer money to false accounts, obtain information on real estate, identities, etc.

Hackers may obtain password, keys, IDs (by way of getting a list of users with all required information, documents, listening of phone talks) and penetrate in computer system as authorised users. Systems with
no authentic identification (e.g. identification by physiological features like fingerprints, eye retina, and voice) are especially invulnerable in this relation. Comprehension of such a modus operandi which keeps on changing with technological advancement shall help in development of law regarding control of cybercrimes.

**Nature of Cyber Crime**

The term ‘cyber’ is derived from the term ‘cybernetics’ which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crime committed in cyberspace relating to machines or devices or cyber technology related crimes are to be treated as cyber crimes. Information technology and electronic commerce are widely used to facilitate crime or to commit crime. In wider sense cyber crime is a crime on the internet which includes hacking, cyber theft, forgery, flowing of viruses, cyber pornography.

“It is very essential to emphasise here that the world is not run by weapons any more, or energy, or money. It is run by ones and zeros……little bits of data……. it is all electrons. There’s a war out there, a world war. It’s not about who has the most bullets. It is about who controls the information”.

Cyber crimes are computer related as well as computer generated crimes. This is increasing every moment which is the cause of global tension. Therefore, law agencies must have detail knowledge and understanding about varying nature of cyber crime.64

---

Cyber crime is a threat to national and international socio-economic, political and security system.\textsuperscript{65} According to loader B.D., a flexible communication system designed to withstand attack by means of rerouting message has also proved difficult for government to control. Sources of illegal activity often require advanced computer skills to be detected as a consequence of their anonymous character.\textsuperscript{66}

**The Concept of Cyber Crime**

Computers do not commit crime.\textsuperscript{67} But computers may be a medium or an instrumentality to committing even traditional crimes. Cybercrime, computer crime, computer related crime, e-crime and hi-tech crime are different names of the same criminal activity. In fact, cybercrimes is a misnomer – it is the slang given to any activity of criminal nature with respect to computer and the Internet. The concept of cyber crime has been a subject of debate for over 30 years. Just as a precise definition of crime does not exist, the concept of cyber crime also demonstrates the same illusiveness to an exact definition. The concept has been long associated with computers storing data in binary. The networking of computers and the case with which the data could move on a network has changed the meaning of cyber crime, even at the conceptual level.

Stanford Research Institute (SRI) was first to suggest a prototype in 1973\textsuperscript{68} which has by and large been followed by writers on cybercrime.

\textsuperscript{66} Ibid.
\textsuperscript{67} Donn Parker, a retired guru, however, anticipates a day of “automated crime” when a software package will be available which when put to use will automatically select the victim, anonymously commit the crime and remove the evidence of its commission from the computer. Donn B. Parker, ‘Automated Crime’ in Cybercrime, International Conference Course Book, Oceana Publications, Washington, D.C. 1997.
\textsuperscript{68} Donn B. Parker, S Nycum and S.S. Oura, Computer Abuse (Mento Park., California Standford Research Institute, 1973).
The organizing schema suggested was; the computer as a subject of a crime; the computer as an object of a crime; or the computer as instrumentality. The increasing use of other devices like the cell phone or PDA required reformulation of the concept. The evolving definition of cyber crime needs to accommodate the mobile phone broadband communication, wireless networks and the Internet. The definition should accommodate both current and emerging technologies.

Some writers have made modification at the conceptual level. According to them, a useful reformulation of this conceptual model is to regard computer-related crime as a conduct proscribed by legislation and/or jurisprudence that (a) is directed at computing and communication technologies themselves; (b) involves the use of digital technologies in the commission of the offence; or (c) involves the incidental use of computer with respect to the commission of other crimes, and hence the computer as a source of evidence.69

Scope of Cyber Crime:

In 1987 the American Bar Association conducted a survey of three hundred corporations and government agencies regarding the concept of computer crime and their resulting loses. 72 of the respondents claimed to be the victim of computer-related crime within the past 12 months, experiencing loses estimated to range from $145 million to $730 million.70

In 1991, a survey of computer related crime of 3,000 Virtual Address Extension sites in the United States, Canada, and Europe was

conducted. 8% of the respondents were uncertain whether they had experienced a breach of security incident that had been a criminal offense. 72% of those who responded said they had been the victims of computer-related crime within the past twelve months.71

In October 1992, at the international level, the Association International de Droit POnal (“AIDP”) held the Colloquium on Computer Crimes and Other crimes against Information Technology in Wartzburg, Germany. The AIDP released its report on computer crime at the conference. The report was based on other reports received from its member countries. The report stated that less than five percent of computer crime was being reported to law enforcement authorities.72

Criminologists use the term “dark figure” to refer to undiscovered computer crime. Several factors contribute to this dark figure.73 These are as follows-

1. The operational speeds and storage capacity of computer hardware makes criminal activity very difficult to detect.
2. Law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data processing environment.
3. Many victims of computer crime have failed to create contingency plans to deal with computer crime.
4. Once criminal activity has been detected, many businesses have been reluctant to report criminal activity because of fear of adverse

71 Ibid.
72 United nations, supra note 41, at paragraph 27.
73 Ibid. at paragraph 30.
publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions.\textsuperscript{74}

**Reasons of Cyber Crime**

Hart in his work “The Concept of Law” has said “human begins are vulnerable so rule of law is required to protect them”.\textsuperscript{75} Applying this to cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reason for the vulnerability of computers may be said to be:

a. **Capacity to store data in comparatively small space**

The computer has unique characteristic of storing data in a very small space. A small micro-processor computer chip can store lakhs of pages in a CD-ROM. This storage capacity\textsuperscript{76} had enough space to remove or derive information either through physical or visual medium in a much easier ways. Any data stored in ROM\textsuperscript{77} will remain intact even if the power is turned off. Whatever be the type of ROM used, the data stored therein is non-volatile and will remain so indefinitely unless it is intentionally erased or overwritten.\textsuperscript{78}

b. **Easy to access:**

The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice

\textsuperscript{75} Hart H.L.A: The Concept of Law, p-73
\textsuperscript{76} The Storage Capacity is measured in terms of “bytes”, “megabytes” and “kilobytes”. Kilo stands for 1000, one mega bytes equal to about 500 pages of the text.
\textsuperscript{77} ‘ROM’ stands for “Read only Memory”. Thus, it is a type of memory that can hold data permanently or semi permanently.
recorders, retina images etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

c. Complex:

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

d. Negligence:

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

e. Loss of evidence:

Loss of evidence is a very common and obvious problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses this system of crime investigation.  

Aspects of Cyber Crimes

There are following aspects of cybercrime:

(a). Technological Aspect of Cyber crime

From a technological dimension, other experts point out the need for a comprehensive term, such as "electronic crime" or "e-crime", thanks to the convergence of ICT, including mobile technology, telephony,

memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included.

(b). Anthropological Aspect of Cybercrime

From an anthropological aspect, cyber crime originates from various populations and exhibits socio-educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. The maladjustment of the education system may contribute to the development of new forms of cyber crime or deviant practices and behaviour with various levels of severity, including cheating and reputational damage, which can be related to frustrations and the redefinition of material and citizen values, inconsistent with what is expected when approaching and leading an adult life. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred. With regard to techno-ideological factors, one must consider sites and networks aimed at propaganda, destabilisation, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

(c) Strategic Aspect of Cybercrime

From a strategic aspect, cyber crime is seen as an offense to cybersecurity, namely attacks to digital networks for the purpose of seizing
control, paralysing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

**Impact of Cyber Crime**

This section presents the results concerning the impact of technological change and breakthroughs of dominance – or rather, of the increase – of cyber crime during the 2010 to 2020 decade.\(^8\)

(a). **Perception of the Impact of Cybercrime:**

The impact of cyber crime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap between lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. However, its use can be described as negative or positive. This is especially true in cryptography, used for securing transactions and data interchange as well as to secure communications covering illegal activities and the establishment of evidence. History shows that new technologies, rarely regulated and not fully complete, are both used for good and bad.

The next ten years will be marked by mobility, with the need for availability, real-time communication, connectivity, and a dependence on digital identity equipment and risk. This decade will also include monitoring automata systems and increasingly new risks.

---

(b) **Negative Developments with regard to Cybercrime:**

Expected developments, which may have a negative impact on cybercrime, render little distinction between work life and private life, using for example the difficulty of locating information for a company and Web applications with cloud computing, targeted stealth malware, and more generally, the massive use of new technologies, including mobile and wireless technologies, and a careless exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past. We must emphasize the volatile nature of finding data as evidence and the difficulty of reporting offenses to the sources, with no legal means, because cybercriminals are adapting alongside new technologies.

(c) **Positive Developments with regard to Cybercrime**

Security measures based on these same technologies could have a positive impact. Security is central to the problem and must be based on policies and be strictly enforced. It will be a major challenge with cloud computing, due to the complexity of where data is stored and the numerous jurisdictions involved, major risks associated with governance and territoriality. The effective level of quality security will be a key factor in the acceptance of these new services.

**Unique Features of Cyber crime**

Computer crime may be committed breaching the user’s privacy without reaching the victim. There is no sign of any kind of violence or struggle at the scene of crime, which are usually the elements of a traditional crime. Cyber crime may be committed by a mere click of the mouse without the knowledge of the victim, thus leaving him totally
incapacitated. In many cases, the victim even does not know that he has been subjected to a cyber crime and become a victim of it.\textsuperscript{82}

Computer crimes have some unique and peculiar characteristics which may briefly be stated as follows:

1. Computer crimes have now become a global phenomenon which does not have any territorial barriers or jurisdictional restrictions.

2. Another peculiar feature of a cyber crime is non-existence of any physical evidence of it. Unlike a traditional crime, where the evidence can visibly be seen and felt in the form of weapon, blood stains, fingerprints, DNA etc. the cyber crime does not leave any such physical evidence to indicate its occurrence. The evidence in case of cyber crime being in the digital format can be identified only by specially trained and skilled computer users.

3. The perpetrators of cybercrimes are generally highly intelligent educated person who cherish a challenge. They are well conversant with the operation of the computer system and its intestacies. A person without adequate knowledge of working of the computer system and internet cannot commit such crime.

4. Some of the cyber crimes are not really new in substance, but the medium through which they are committed is new, whereas others represent an altogether new form of illegal activity. Some of the newly emerged cyber crimes are electronic vandalism, cyber terrorism, transnational crimes in cyberspace etc.

5. The medium for cyber crime being computer network system, it does not require the user to disclose his identify. Thereafter, a cyber

\textsuperscript{82} Vishwanath Paranjape: Cyber Crimes and Law, Edn. 2010, Central Law Agency, p-24
criminal can conveniently manage his anonymity, which enables him to remain out of reach of the law enforcement agencies.

6. The computer network has created new potential to commit traditional crime in non-traditional ways. For example, cyber terrorism, cyber fraud, money laundering, theft of data, cyber pornography, counterfeiting by using computer etc. are some of the traditional crimes which are now committed on-line through electronic media.\(^{83}\)

**Stages of computer crime:**

In general penal code, there are four stages for commission of an offence is intention, preparation, attempt and commission. Similar to this, there are also stages in the commission of a computer crime. K.P.C. Gandhi in his article “An introduction to computer related crime”\(^{84}\) suggested the four stages in the commission of computer crime viz.-

a. **Planning:** Most of the computer crimes are not spontaneously done but carefully planned often for extensive periods. For this purpose, the criminal acquires certain information such as data entry practices programme listings, systems documentations, locations of the system, access and system security procedures.

b. **Execution:** Execution of computer crimes differs from execution of other crimes. The presence of the perpetrators is not necessary for the computer crime to be committed. There are different methods for commission of computer crime such as using terminals or

---

\(^{83}\) Extracted from inaugural address delivered by Shri S.P. Talwar, Deputy Governor, Reserve Bank of India, in the National Seminar on Computer Related Crime, organized by CBI, New Delhi on February 24, 1999.

communication channels to gain access, modifying application programmes or operating system, entering extra or modified transaction to an input file, physical removal of programmes or data, accessing controlled information and copying the same, physical actions such as arson or theft and manipulating the actions of programmes or people.

c. **Concealment:** Once the crime has been committed, the tendency of the criminal is to remove traces of crimes. There are several ways to hide the crime including representing the crime as an error or omission in an otherwise normal run, representing a fraudulent transaction as a normal transaction being executed, modifying an individual account but manipulating the systems totals to reflect normal result, misrepresenting a criminal activity as an error of flaw within a system and performing the illegal act in conjunction with an authorized activity.

d. **Conversion:** Once the crime has been committed, the immediate problem for the criminal is to convert the asset into a more useful form. Conversion may takes forms such as sale of data unauthorisely acquired, destruction of data in cases of revenge, or in most of the cases for financial gain.

**Challenges of Cyber Crimes**

Cyberspace does not recognize geographical boundaries. This has proved a boon to the delinquents who perform illegal activities on the Internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the part of law enforcement
agencies further complicates the matter.\textsuperscript{85} The challenges posed by Cyber crimes are classified as;

i. Legal challenges which are dependent on the statutory provisions to be used as a tool to investigate and control the Cyber crimes.

ii. Operational challenges require a cohesive well trained and well equipped force of investigators operating and coordinating at national and international level.

iii. Technical challenges thwarting the efforts of law enforcement agencies’ ability to catch and prosecute the online offenders.\textsuperscript{86}

Cyber crimes are often committed beyond the national borders. The national standards of criminal behaviour vary. Furthermore, it is very difficult to identify the perpetrator of wrong because Internet facilitates anonymity. Thus, cyber crimes pose challenges that are unique in character unlike traditional crimes. These crimes cannot be effectively dealt with by simply passing national legislation. The IT Act has extra-territorial jurisdiction and applies to any offence or contravention thereunder committed outside India by any person.\textsuperscript{87} This feature of the IT is not unusual. Similar provision is found in the IT legislations of other jurisdiction also.\textsuperscript{88}

\begin{flushleft}
\textsuperscript{85}Farooq Ahmad: Cyber law In India (Law on Internet), Edn. 3rd, pp-371-37
\textsuperscript{87} Section 1 (2) and Section 75
\textsuperscript{88} Section 4 of the British Computer Misuse Act, 1993 (as amended 1998) and section 9 of the Malaysian Computer Crimes Act, 1997
\end{flushleft}
However, this provision can be effective only when there is a mutual cooperation at the international level amongst the enforcement authorities and Governments. 89

Motives of Cyber Crime:

Generally motives for cyber crime are same as in conventional crimes. These motivations may include economic – personal benefit and financial gains, revenge–desire to inflict harm, adventure–challenge of mastering a complex system, to impact large system and organizations; ideology desire to express and protest and lust of self-aggrandizement and/or self-gratification.

The Target of Attack:

The target of attack is a computer, computer system, computer resources of communication devices containing information resources which includes data, text, images, sound, codes, computer programmes software and databases. Computer data are typically stored in billions of files in a global network of computers. The information so stored has value for those who get access to these files. The target of attack, being the data/information, is intimately connected with the value of information to the attacker. Technologies have you to be developed to provide absolutely safe and secure systems of storage and transmission of information. The systems are vulnerable and there are people who are motivated to do bad things. Until a safe and secure system is evolved, an unwelcome intruder will remain inevitable in an environment of uncertain future.

89 Supra note 16 at 123.
a. **The Attackers:**

The persons who attack the information resources in computer system are individuals and entities who use computers as a victim or as an instrument to secure, manipulated or modify information and databases. They are not necessarily individual hackers alone; even governments and corporations may intrude and penetrate into the databases of other seeking there from military or economic intelligence. These intruders may be described as insider, hackers, criminals, terrorist, corporations and governments.

b. **Insider:**

The insider is a present or former employee in the government or commercial organization. Divulgence of information may put the interest of the organisation in serious jeopardy; even put them to irreparable loss. The information to which they have access has a market. In today’s competitive commercial world, rival companies are willing to pay just any price.

c. **Outsider: Hacker:**

He is person who gets unauthorised access to computer or communication device. Hackers can break into a computer in a variety of ways. They can draw on numerous software tools. There are numerous web sites and FTP servers which make available such software. They are increasingly and even by inexperienced hackers to break into the system hacking tool-kits are available for a price.90

---

d. Individual Criminal and the Criminal Organisations:

Most of the activities of hackers are criminal in nature. *Phishing and Identity theft* are interrelated activity with a view to gaining access to another person’s identification information, like name, social security number, driving licence, bank account number and credit card numbers. After securing such information, the thief impersonates the genuine person and takes actions on his or her behalf, such as withdrawing funds, borrowing money and charging purchasers. The criminal organizations have now specialised in developing crime ware which are offered for sale with a price. They are getting better and better at protecting themselves from the long arm of the law by using *crime-ware services*. The operator does not conduct the criminal activities himself but only provide the infrastructure for conducting such activities.91

e. Botnets:

Internet bots (derived from the word web robots) are software applications that run automated tasks over the Internet. They are used for both commercial as well as malicious purposes. Hacker bots brows the Internet looking for system with exploitable vulnerabilities. The word botnet is generally referred to compromised computers (called *zombie computers*) running software, like worms, Trojan horses or backdoors usually installed by exploiting Web vulnerability giving the owner of the botnets control of compromised computers under a common command – and – control infrastructure. The compromised machines are referred to as drones or zombie, the malicious software running on them as ‘bot’. Botnets can be used to engage in Click Fraud, Distributed Denial of

---

Service (DDoS) attacks on other websites/servers of Keylogging or Warez (stealing software and license) and Spam. According to an estimate, India has more than forty commands-and-control servers, and has approximately 38,465 distinct bot-infected computers.\footnote{92. “Bots in hunt for newer prey.” BS Reporters/New Delhi/Mumbai November 02, 2007 [http://www.business-standard.com/india/news/bots-in-hunt-for-newer-prey/302996]}

f. **Terrorists:**

Terrorism refers to actual or threatened use of violence with the intention of intimidating groups, societies or the governments to secure some political or non-political advantages. Much of terrorism is associated with internal warfare or liberation movements. These terrorists group or organisations are increasingly using web media. Often, Internet becomes the life-bood of underground organizations. They are involved in what Barry Collins called ‘cyberterrorism’, a word he is said to have coined. It refers to convergence of cyberspace and terrorism. The ramifications of the potential of cyberterrorism to some terrorist organisation like al-Qaeda are profound. Unsetting signs of al-Qaeda’s aims and skills in cyberspace have led some government experts to conduct that terrorists are the threshold of using the Internet as a direct instrument of bloodshed.

g. **Corporations:**

Countless companies world-wide have shown their presence on the Internet selling their products and services. Stiff competition has led to unfair trade practices and also cyber crime such as theft of trade secrets. These activities may be classified as Industrial espionage. Rival companies are willing to pay just any price for industrial espionage.
Criminal organisations often step in to provide that information which criminals secured via their Trojan horse.

h. Government and Foreign Agencies:

Almost every country has an intelligence agency that collects information about foreign allies and adversaries including foreign allies and adversaries including foreign governments, terrorist organizations and other threat to national security. They also use electronic surveillance including even computer hacking.\textsuperscript{93} Besides intelligence, Governments also target economic and trade secrets in order to boost and protect their economies.\textsuperscript{94} Hackings and DDOS attacks by foreign governments may be called as \textit{Cyber warfare}.

Tools and Techniques of Cyber Crime

Tool and techniques of cyber crime are as follows\textsuperscript{95}:

(i) Unauthorized Access: Access\textsuperscript{96} is defined as ‘gaining entry into instructing or communicating with the logical arithmetical or memory function resources of a computer system or computer network’. 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 system or computer network. Thus not only would accessing a server by cracking its password authentication system be unauthorized access. Packet sniffing tempest attack password cracking and buffer overflow are common techniques used for unauthorized access.

\textsuperscript{93} Dorothy E. Denning. Information Warfare and Security (New York, AMC Press, 1999), p 6
\textsuperscript{94} Id. at p. 63.
\textsuperscript{95} N. Muddaraju and Ramesh: Cyber Crimes: need Effective Law, Cri LJ August 2009 Journal Section.
\textsuperscript{96} Section 2(1)(a) of the Information Technology Act, 2000.
(ii) **Packet Sniffing:** Packet Sniffing is a technology used by crackers and forensics experts alike. To understanding Sniffing the need is to first understand the basics of data transmission. It’s a known fact that data travels in the form of packets on networks. These packets also referred to as data-grams are of various sizes depending on the network bandwidth as well as amount of data being carried in the packet in the measure of bytes.

(iii) **Tempest Attack:** Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct the data\(^\text{97}\). This allows remote monitoring of networks cables or remotely viewing monitors.

(iv) **Password Cracking:** A password is a type of authentication it is a secret word or phrase that a user must know in order to gain access\(^\text{98}\).

(v) **Buffer Overflow:** Also known as buffer overrun input overflow and unchecked buffer overflow this is probably the most common way of breaking into a computer.

It involves input of excessive data over flows into other areas of the hacker to insert executable code along with the input thus enabling the hacker to break into the computer.

\(^\text{97}\) Information Technology Act, 2000, Sec 2(1) (o) “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.

\(^\text{98}\) Information Technology Act, 2000, Sec 2(1) (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 system or computer network’.
(vi) **Viruses:** A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a possibly evolved copy of it.

**Categories of the Cyber Criminals**

A microscopic analysis of the trends in the cyber crime would lead us to believe that the cyber criminals could be broadly categorized under two categories sharing different ideologies and the mode of operation differs as well. They are idealist and greed motivated. The idealists want to hog the limelight by executing their evil intention in such crafty manner with cunningness so they won’t be traced. Their actions are usually confined to hacking of the secured computer systems as well as spreading highly detrimental virus which could damage the security of the country.

The greed motivated as the name suggests are fascinated with the intention of earning money and they are hell bent upon finding some means and ways through which they could get some pecuniary benefits by resorting to certain fraudulent means. Now moving bad to worse, the modern trend portrays even a more dismal scenario wherein the computer is used as an arsenal to execute the draconian plan of organized means so as to trespass the intelligence in materializing the plans with utmost clinical precision. However the action of the idealist are not damages, the denial of service that is said to have inflicted heavy damages.\(^9\)

**i. Cyber Criminals who use computer as tools of crime:**

The Mellisa and I love You virus which spread like wildfire were instrumental in breaking the backbone of the United States economy

---

\(^9\) Vogel Joachim, Towards A Global convention Against cyber crime, First World Conference on Penal Law in the XX1 century, Guadaljara Mexico, 18-23 November, 2007
by inflicting pecuniary loss to the tune of I billion dollar of damages. One of the unique aspects is that most of the attacks launched by the teenagers are comparatively less detrimental to the individual at the micro scale but are highly damaging to the society at large at macro scale.\textsuperscript{100}

The greed motivated criminals could be articulated as the carrier criminals with criminal track record. They would have already perpetuated a lot of anti social activities. They would have carved out a niche for themselves for their notorious acts. They are indulged in atrocious acts of the child pornography which is making geometrical progression in the United States of America. This has undermined the human dignity and often considered as the blatant violation of the human rights which is considered as an inalienable right of human being.\textsuperscript{101}

\textbf{ii. Cyber Terrorists:}

They are the most lethal categories of the culprits whose action have alarmed the international community. They believe in sending shockwaves down the spine by launching a well coordinated plan to break upon the security of the country. The penetration into the federal agency computer server National Security agency and the Department of Defense shows the fragility of the national infrastructure and the intelligence when it comes to taking precautionary measures. Osma Bin laden, who clinically executed one of the most dastard attacks in the history by demolishing the Pentagon like house of cards is said to have possessed own satellite communication. He happens to be one of the most

\textsuperscript{101} Digital La Costa Nostra, The Computer Fraud and Abuse’s Act’s Failure to Punish and Deter Organized Crime.
wanted terrorist in the lists of the FBI and was gunned down by the Seal Commando operation in Pakistan.

iii. Mosaic Theory: An Effective Tool in Investigation Analysis:

The Mosaic Theory emerged as a specific branch of study after the heinous act of 26/11 where there was a huge devastation of lives and property in the United States masterminded by Osama Bin Laden. It is a theory of informational synergy. It describes a process through which adversaries collect, combine and compile items of information some or all of which are harmless in their own right. This theory believers that if it is required in the interest of the security of the country at large than the classified information of the Government could be utilized for making the investigation process more transparent and effective. The FOIA opinion recently stated that the idea behind adoption of this technique is to assemble discreet information into something concrete.

The theory faces a daunting task in the way of reconciling between the principles of openness and transparency with those other social and Constitutional goals of preserving the confidentiality of the sensitive commercial and personal information.

iv. Electronic Pearl Harbour: Cyber Terrorism could create Havoc warns Richard Clarke:

Richard Clarke, who has been involved since long in the counter terrorism and cyber security has served in many pivotal post in the United States. He had served as national coordinator for security infrastructure protection of counter terrorism on the National Security Council.

102 Growing Global Threat of Economic and Cyber Crime, The national Fraud centre in conjunction with the Economic Crime investigation Institute, A Lexis Nexis Company
According to Mr. Clarke America built cyber space and it must defend cyberspace. Mr. Clarke said accepting his new position. Since years, he has been warning the world about a lethal and organized act of terrorism referred to him as Electronic Pearl Harbour which is a computer based attack that would cause massive amounts of destruction and loss of lives.

In a worst-case scenario such an attack would target power distribution, financial services, emergency call services and air-traffic control systems. Concerns have been raised from all quarters regarding the vulnerability of the unguarded cyberspace. It is believed that the hijackers who took part in the attacks on 11 September are believed to have used the internet to communicate, often logging on at terminals in public libraries and copy shops to make their online activities difficult to track.\textsuperscript{103}

v. \textbf{Internet Criminals: Spreading the corporate hoax to gain from such speculations:}

There are particular classes of cyber criminals who are only concerned about spreading the hoax regarding the share value of a particular company. They really count on the fact that investors should repose faith on their statements and act according to their deceptive designs. In caser everything works out according to the scheme of plan, then the criminals would be likely to be benefitted to the tune of crores of rupees. There are a plethora of instances where the cyber criminals have craftily deployed this plant in order to materialize their evil designs.

It is very difficult to categorize these criminals within the water compartmentalized manner as they commit crimes as stock brokers

\textsuperscript{103} US names Cyber Terrorism Czar, Available at http://news.bbc.co.uk/2/hi/americas/1590398.stm, accessed on 15-8-2009.
utilizing computer as the media to spread the wrong message throughout the globe. They have tremendous idea about the stock market and they understand the fact the entire stock market runs on speculations. Therefore this message spreads like wildfire across the forest.

vi. Miscreants misguiding the businessman through hoax:

In August 2000, one miscreant sent hoax that Emulex, a Company listed on the NASDAQ stock market was experiencing huge losses and that the forecast for the next quarter is so much so bleak that the CEO is resigning. Traders who follows all information very meticulously, reposing trust information published in the financial networks immediately sold the massive stock which dropped more than 5$ in market value. Within a very short span of thirty minutes Emulex recovered from the loss. A miniscule span of thirty minutes was sufficient for the criminal to accumulate money to the tune of $250,000 by misguiding the customers of the stock market. There was imminent apprehension that the hoax might have been spread by the company itself to recover from the financial crisis which on investigation transpired to be false. But police nabbed the miscreant a few days after.104

vii. Cyber Criminals targeting the social networks: Exploitation of the unguarded cyberspace:

It is not just the average net user who is a fan of social network sites, so are hi-tech criminals. Internet criminals are being increasingly drawn to social networks like Face book and My Space due to the relative ease of gathering personal information. Koobface, a potentially dangerous virus is perpetuated through face book. It sends the victim a warning that

104 Cyber Crime Fear and Victimization: An analysis of a NATIONAL SURVEY BY Abdullah Allsahan, A Dissertation paper submitted for the Degree of Doctor of Philosophy in Sociology in the Mississippi State University, may 2006.
its Flash player is outdated along with an invitation to download a new version, which is in fact the virus. The chances of the virus being proactive in the social networking site are rather more due to the fact that there is lot of applications which includes quizzes games and other tools that can disguise links to malware sites.\textsuperscript{105}

The vulnerability of social networking sites was underscored in a study by security company Sophos. A vicious virus Koobface “koob” being “book” in reverse has affected thousand Face book and Twitter users since August 2008, said Asier Martinez, a security specialist at global IT solutions provider Panda Security. The virus hijacks the accounts of social networking site users and sends messages steering friends to hostile sites containing malware, malicious software often designed to infiltrate a computer system for illicit purposes. Real cyber-crime mafias have now taken over, especially in Russia, China Brazil and the Ukraine whose goals are purely economic gain, she said, underscoring that hacking could be highly lucrative.

There has been lot of studies going on across the globe to quarantine the virus which is spreading like wild fire across the forest through the social networking sites. The mischievous design of the cyber criminals is quite apparent on the face record and needs no in-depth research. David Porter, head of security and risk at Detica, said the apparent familiarity of social network sites, which often help people build connections with people who share their interests and outlook, meant many people were cavalier with their personal information.

Face book says that less than 1 percent of its have been affected by a security issue, such as a virus, since the site opened in 2004. Garcia said

\textsuperscript{105} Vakul Sharma: Handbook of Cyber Law (Macmillan) 2002, P.- 93.
the number of viruses detected in recent years has exploded while the profile of cyber-criminals has changed. “Before it was very savvy teenagers who wanted to show off their computer skills. Now you don’t really need to know much about information technology to be a hacker, all the tools have already been created”, she said. Face book has sought to resist attacks by Koobface and similar viruses by blocking links to hostile sites and shutting down accounts from users that show signs of infection, such as sending too many messages.  

The Ten Commandments of Cyber Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people’s computer work.
3. Thou shalt not snoop around in other people’s computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people’s computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people’s intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.

106 Harmonizing Legal Response to Cyber Crime: A Global Concern, visited on 10/13/2010, 6:35 A.M
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.\textsuperscript{107}

**B. Typology of Cyber Crimes**

Cyber crime is only a generic term that is used to denote the criminal activities in which a computer or a computer network is either the instrumentally for its commission or its target. It is not easy to fit them under straightjacket types and categories. Many of the cybercrimes could easily fit into different types. For example, a computer fraud is at the same time affecting an individual who has been the victim and the economy in general. Hacking is a crime that uses computer as a tool and also as a target. Cyber crime is dynamic and the criminals innovate their activity on a daily basis.\textsuperscript{108}

The classification of cyber crime can be classified on various criterions, such as the typology of cybercrimes on the role of computer as an object as well as a tool for its commission, typology based on the criteria of the victims of the cybercrime, typology based on the categories of the offenders and finally the typology of cyber crime on the basis of the content, which brings within its fold almost all the cybercrimes. Except this typology other classifications of the cybercrimes are being treated here briefly. However, the individual cyber crime will be given exhaustive treatment under the last category of the cybercrimes, i.e., content based typology.

\textsuperscript{107} The computer Ethics Institute, a leader in the field, has comprised a guideline to help computer users in their ethical decisions. They have called this guideline “The Ten Commandments”. Charter David L Computer Crime Categories – HOW TECHNO-CRIMINAL OPERATE. FBI Law Enforcement Bulletin, July, 1995.

1. Typology based on role of computer in cyber crime:

The typology of cybercrimes can be divided into four general categories on role of computer as below. These are not watertight categories as many cyber activities may fall under one another:

(a) Computer as the Target:

Instances of this category are: when a private or official computer system is attacked by intruding into it through Internet either manually or by other means. This activity generally called, hacking, may involve erasing of data or program, virus and worm attack, logic bombs, infecting computer with Trojan horses, defilement of web site, stealing of data, identity theft, phishing, pharming, denial of service attack, botnet, spoofing, social engineering, malware, vulnerability exploitation and terrorist activity threatening the critical infrastructure.

b. Computer as a Tool:

Computer is used to commit traditional crime in a high-tech manner. E-fraud, embezzlement, forgery, black mailing, sedition, promoting enmity between different classes, and defamation may be committed digitally. Other crimes committed on the internet, theft of intellectual digital property, stalking, gambling and money laundering. Beside these, there are numerous other undesirable activities involving the internet.

c. Computer as incidental:

The third category relates to situation where use of computer by a criminal is incidental. It may be used as a storage device. Here computer is not needed for the criminal activity but may provide evidence of the
crime committed. Examples include personal and financial records of a person involved in economic and financial crimes. Notes maintained by a drug trafficker or a person belonging to a terrorist group. Information contained in the computer is of high evidentiary value in any prosecution for the crime. Computer generated data and records hidden in the hard disk of the computer or other saving devices like floppy disks and compact disks (CD/DVD) are relevant not only in cases where computer is used as incidental to a crime but also afford evidence of cyber crime.

d. Computer as Associate:

Yet another type of crimes that falls under the purview of cybercrimes is the new versions of traditional crimes that across as a result of widespread increase in the availability of computers and information technology. Software piracy is an ideal example of this type of crimes. It is only because there is a ready market due to large numbers of computers, that software piracy takes place. In this type of cybercrimes, technological growth essentially creates new crime targets. Counterfeit, copyright violations, theft of computer accessories, piracy in audio and video market etc are some examples of this type of crimes. As the Internet and computer increase their presence in the global society, this type of cyber crime is expected increase phenomenally over the coming years.

2. Typology based on perpetrators of cybercrime: Insiders vs. Outsiders:

a. Insiders:

Another way of classifying cyber crimes is on the basis of the profile of criminals. Some studies indicate that nearly 75% of the
cybercrimes are committed by the insiders like employees. It may range from using the organisation’s computer for personal purposes to causing serious damage to the system by some disgruntled employee. Almost every organization faces the problem of computer abusers who use their time to surf, chat or do other personal things, whereby the productivity is affected. Typical insider crimes include missing parts and software, improper logon attempts including using of other people’s identity and password, subverting the payroll system for personal benefit etc.

b. Outsiders:

Most common outsider threats originate from Hackers. Though, initially, it was more like fun and challenges to break a password and enter another person’s computer system, lately using of hacking for more serious crimes is on the increase. The intelligence agencies all over the world has realized the potential of cyber espionage as use of computer networks for data collection and management has become inescapable. Industrial espionage involving competitors are also on the increase.

3. Typology based on victims of cybercrime:

Another typology that has been used is based on the targeted victims of the crimes. The types identified under this method are briefly discussed below-

i. Against Individual:

(a) The person and

(b) The property of an individual
ii. Against Organizations:

(a) Government

(b) Firm, Company, Group of Individuals

iii. Against Society at large:

The following cyber crimes are committed against the following groups:

**Against Individuals:**

(i) Harassment via e-mails.

(ii) Cyber-stalking.

(iii) Dissemination of obscene material.

(iv) Defamation

(v) Hacking/cracking.

(vi) Unauthorized control/access over computer system.

(vii) Indecent exposure.

(viii) Email spoofing

(ix) Cheating and Fraud.

**Against Individual’s Property:**

(i) Computer vandalism.

(ii) Transmitting virus.

(iii) Netrespass.
(iv) Hacking/cracking.

(v) Unauthorized control/access over computer system.

(vi) Intellectual Property crimes

(vii) Internet time thefts.

**Against Organization:**

(i) Hacking/cracking.

(ii) Unauthorized control/access over computer system.

(iii) Possession of unauthorized information.

(iv) Cyber terrorism against the governmental organization.

(v) Distribution of pirated software etc.

**Against Society at large:**

(i) Pornography (basically child pornography).

(ii) Polluting the youth through indecent exposure.

(iii) Trafficking.

(iv) Financial crimes.

(v) Sale of illegal articles

(vi) Online gambling.

(vii) Forgery
4. Content Basis Typology of Cybercrime

The *modus operandi* of committing the cybercrimes is different than the traditional crimes. However, sometimes conventional crimes are committed by using computers. Besides committing the cybercrimes through the instrumentality of computer, there are certain pure cybercrimes which are committed only in the cyberspace. The attempt of the researcher would be to enumerate a comprehensive list of the various types of cybercrimes which are being committed in the recent times. Various categories of cybercrimes are as follows:

a. Hacking:

Hacking means unauthorized access to a computer system.\(^{109}\) It is the most common type of Cyber crime being committed across the world. The word, hacking has been defined in section 66 of the Information Technology Act, 2000 as follows, “whoever with the intent to cause or knowingly that he is likely to cause wrongful loss or damage to public or any person, destroys or alters any information residing in computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking”

Hacking is one of the most common cyber crimes committed mostly either for fun by the teenagers or to cause harm and earn some profit by stealing private information like credit card numbers, account numbers, confident information stored either in emails or in the hard disk of computer for terrorism etc.\(^{110}\)

---

Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend up to two lakh rupees or both.

The Indian law has however given a different connotation to the term hacking, so we do not use the term “unauthorized access” interchangeably with the term “hacking” to prevent confusion at the term used in the Act of 2000 is much wider than hacking.

**Instances:** On 9th June 2005, hackers attacked on one website in Baroda, Gujarat and claimed $10,000 for restoration of website.\(^{111}\) Indian Police even become vulnerable. They found out no clue to control the incident. Domain name was the issue. The “website” which might had been kept unlocked with registrar was fraudulently transferred and controlled by hackers. Therefore, it is very vital to see the standard of security system of the domain name which any one is going to buy from any company or institutions.\(^{112}\)

**Kinds of Hacker:**

There are following kinds of hackers:\(^{113}\)

i. **Code Hackers:** They know computer inside out. They can make the computer do nearly anything they want it to.

ii. **Crackers:** They break into computer systems. Circumventing Operating Systems and their security is their favourite pastime. Das

\(^{111}\) R. Raghavendra, TNN reported in the Times of India, 14th May 2005.
\(^{112}\) M. Dasgupta: Cyber Crime in India (A comparative study), 2009, p-93.
iii. **Cyberpunks:** They are the masters of cryptography.

iv. **Phreakers:** They combine their in-depth knowledge of the Internet and the mass telecommunications systems.

More than 1000 government websites belonging to various Ministers and Departments were hacked in the last three years. Minister of States for Home RPN Singh said as per information reported to and tracked by Indian Computer Emergency Response Team (CERT-in), a total of 303 in 2010, 308 in 2011, 371 in 2012 and 48 up to March 2013, government websites belonging to various Ministers and Departments were hacked. “Department of Information Technology has taken necessary preventive actions,” he said in a written reply in Lok Sabha. Mr. Singh said the preventive actions includes proper audit of all new government websites and application with respect to cyber security prior to their hosting. “It has been mandated that all government websites are hosted on infrastructure of National Informatics Centre, Education and Research network or any other secure infrastructure service provider in the country,” he said.  

b. **Malicious Programs**

Malicious programs such as virus, worms, trojan horses, logic bombs, hoaxes etc. intend to cause harm to its victims.  

I. **Virus:** A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programme like word processors or spreadsheets or they attach themselves to the boot

---

114 1030 govt. websites hacked in the last three years- THE HINDU, May 7, 2013.
sector of a disk. Thus when an infected file is activated, the virus itself is also executed. Section 43(c) of the Information Technology Act covers the area of introduction of viruses, etc. and shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

**Instances:** The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world’s most prevalent virus. Losses incurred during this virus attack were pegged at US $10 billion.

VBS_LOVELETTER utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The email 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 email 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 email was “kindly check the attached LOVELETTER coming from me”.116

Viruses are also classified according to their activity:117

(i) **Boot:** This virus infects the boot sector of a hard disk or floppy. The boot sector is the first sector of the hard disk or floppy disk. It contains important information that is necessary to load the operating system into the memory of the computer. The boot virus loads into the memory of the computer, which then has trouble starting up.

---

(ii) **Programme:** This virus infects executable programme files, have extensions like .exe, .com, .sys, .drv, .etc. When the programme is executed the virus spreads to the files.

(iii) **Macro:** This virus infects the macros of document and templates of MS Word (a part of MS Office programme). When documents are opened the virus activates and sometimes it alerts the text. If this document is copied to another computer through a network or floppy, the virus travels alongwith the document and infects other computer also.

(iv) **Worm:** This is a code that replicates itself without any host programme. Worms are found in networks where they infect all the computers connected to the main server. Worms are very active in the internet.

(v) **Zoo:** A virus created in a computer research lab for testing purposes. The word zoo means that it is confined to one place and not allowed to run wild and spread.

II. **Trojan horse:** A Trojan horse is defined a “malicious, security-breaking program that is disguised as something benign” such as a directory lister, archiver, game, or a programme to search or destroy viruses.¹¹⁸ Trojan let a hacker access the victim’s hard disk, and also many functions on his computer.

III. **Logic bombs:** Logic bombs, once detonated in a computer, makes the program to go into an infinite loop, crash the computer, delete data files, or some other damage to the computer or its data.

¹¹⁸ The word, Trojan Horse is generally attributed to Daniel Edwards of the NSA. He is given the credit for identifying the attack from in the report, Computer Security Technology Planning Study.
IV. **Worms:** Worms are target at the larger machines-most usually, various flavours of UNIX – that are connected to the Internet. These programmes are similar in many ways to the simpler viruses, by infecting series of vulnerable computers. They differ, however, in that they rely on independently propagating copies of themselves to subsequent ‘hosts’, rather than on the actions of unwitting users.

**Instances:** Probably the world’s most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computer had to be disconnected from the network.¹¹⁹

V. **Hoax:** It is false warning about existence of malicious program.

c. **Online Forgery:**

Online forgery is an offence which needs little effort as compared to offline forgery. It is not usually restored to for money but it is also employed for “glory or a spirit of devilment, cocking a snook at experts and purchasers”. Forgery is an offence which existed much before the Internet and in common law, it is defined as fraudulent making or alteration of a writing to the prejudice of another man’s right.¹²⁰ Computer forgery is the alteration of computerised documents. Since the

---

proliferation of high-resolution computerized colour laser copies, a new generation of fraudulent counterfeiting has emerged.\textsuperscript{121}

**Instance:** In October 1995, economic offences wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems. This constitutes forgery using computer.\textsuperscript{122}

**d. Intellectual Property crimes:**

Intellectual property consists of a bundle of rights.\textsuperscript{123} Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc. With the development of internet, such efficient tele-communication and information system has strengthened legitimate commercial activities in the present day fast-paced global market which may also be easily used by the criminal networks. This explosion of digitisation and the internet have further enabled intellectual property violators to easily copy and illegally distribute trade-secrets, trade-marks, logos etc. Intellectual property is physical expression of ideas contained in books, music, plays and computer software. Making copies of intellectual property including music, movies and software without the right to do so is punishable under the Copyright Act\textsuperscript{124} 1957.

\textsuperscript{123} The holder of the intellectual property has certain rights that are vested in him alone, unless he chooses to assign them to someone else.
\textsuperscript{124} Section 2(m) of the Copyright Act, 1957 as amended in 1994 which came into force w.e.f. May 10, 1995.
Instances: In December 2007 Anita Sharma, a former employee of Pune-based 2DPLM Software Solutions was arrested on charges of stealing software source code valued at over INR 48 crore. It was alleged that a few days before quitting her job, she had emailed the source code to her husband. 

   i. Copyright Violation: Copyright is an intellectual property right that subsists in literary and artistic creations. But this right, when violated is not adequately protected and illegal unauthorized distribution of copyrighted works is often the common grievance of copyright owners. A copyright owner may place his work on the world-wide-web with the intention of sharing his creations with the public, but this is usually exploited by the cyber criminals for their personal gain. Besides this violation of copyright plagiarism is also rampant in the academic and literary world, therefore, copyright also seeks protection from plagiarism.

Some aggravated forms of copyright violations are widespread in the business world. They are known as software piracy, industrial piracy etc.

Software Piracy

When a computer operator obtains a copy of the software, he can easily duplicate it without notifying it to the author and sell it for profit. This is termed as software piracy which is a species of copyright violation. This is more or less analogous to making a xerox copy of the

126 The various acts for which copyright Act extends are enumerated in Section 14 of the Copyright Act.

{90}
entire published book and sells it at a significantly low price and earns money.

Instances: Mr. Shanti Bhai had all legal software’s like OS, Office Software, tally etc. in his office. In March 2011, his son was to be wedded so his son thought of making a marriage invitation, existing legal software’s were not suited for making graphical invitations. His friend suggested him to borrow his legal corel draw package and install it on his computer and when the work is accomplished remove the installation. The moment Shanti bhai’s son installed it on his computer and when the work is accomplished removes the installation. The moment Shanti bhai’s son installed the borrowed software on his computer; he committed an act of software piracy.\(^\text{127}\)

**Industrial Piracy:** When an individual or group of individuals attempts duplication and distribution of copyright software for large profits, it is termed as industrial piracy. With the fall in price of the duplication equipments, the incidents of industrial piracy have considerably increased.

**ii. Protection of Trademarks:** Trademarks are those intellectual property rights that protect a trader’s goodwill and reputation and differentiate his goods from other traders in the same streams or business.\(^\text{128}\) Trademark infringement or passing-off actions typically arise through use of marks by one person that belongs to some other person. Thus, if a particular logo is generally associated with and used in relation to product ‘X’, its use by someone else in relation to product ‘Y’, would amount to infringement of trademark

\(^{128}\) Trademark is defined in Section 2(1)(z)(b) of the Trademarks Act, 1999.
right and it would be treated as an act of passing off which is punishable under the law of torts.

e. Cyber Fraud:

The term “cyber fraud” is not defined in the Information Technology Act 2000 in India. However, according to D. Bainbridge, the phrase ‘Computer Fraud’ is used to describe “stealing money or property by means of a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services, or to evade dishonestly some debt or liability. It might involve dishonestly giving an instruction to a computer to transfer funds into a bank account or using a forged bank card to obtain money from a cash dispenser i.e., automated teller machine”.129

As electronic commerce has become more prevalent, the application of digital technology to fraudulent endeavours is much greater. The term computer fraud denotes a sub-class of economic crimes that are being carried out by the help of a computer networks and Internet in the cyberspace.130 Internet has certain inherent features that make it ideal for fraudulent purposes: Cost-effectiveness, breadth of reach, difficulties in authenticating identity, anonymity, ease of personalizing appeals, and novelty.131

Online fraud is one of the most lucrative business that is growing today in cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs etc.

Instances: Recently the court of Metropolitan Magistrate, Delhi, found guilty 24 year old engineer working in call centre, of fraudulently gaining the detail of Camp’s credit card and bought television and cordless phone from Sony website. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating under IPC, but did not send him to jail, Azim was asked to furnish a personal bond of Rs. 20,000, and was released on years probation.132

f. Cyber Terrorism:

Cyber terrorism may be defined to be “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”133. The convergence of Cyberspace and Terrorism is known as Cyber-terrorism. Cyber-terrorism is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a Government or its people in furtherance of political or social objective.134

The role of computer with respect to terrorism is that a modern thief can steal more with a computer than with a gun and a future terrorist may be able to cause more damage with a keyboard than a bomb. No doubt, the great fears are combined in terrorism, the fear or random, violent, victimization segues well with the distrust and out of fear of computer technology. Technology is complex, abstract and indirect in its impact on individual and it is easy to distrust that which one is not able to

132. Mehta Dewang: Role of Police in Tackling Internet Crime (Universla Pub.) 2003 P. 71
control. People believe that technology has the ability to become the master and humanity its servant.\textsuperscript{135}

A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorists' attack on the Internet is by distributed denial of service attacks, hate websites and the emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt.\textsuperscript{136}

Therefore, we can say even use of mobile phone, wireless, laptop, pocket PC as well as traditional concept of computer to commit terrorism or causing injury to those who cause terror in the mind of public and Government will be treated as cyber terrorism.\textsuperscript{137}

**Instances:** In 2001, in backdrop 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 websites, prominently the website of the White House.\textsuperscript{138}

g. **Cyber Warfare:**

The cyber warfare has gained so much favour among the military strategies that most of the Armies world over now have dedicated cyber warfare terms for defensive as well as offensive operations. Defence

\textsuperscript{136} Rahul Mathan: Law Relating to Computers & Internet (Butterworth New Delhi) 2000, P. 173
planners around the world are investing substantially in information warfare—means of disrupting the information technology infrastructure of defence systems.¹³⁹

h. Cyber Pornography:

Pornography¹⁴⁰ is defined as the ‘sexually explicit depiction of persons, in words or images, created with the primary, proximate aim, and reasonable hope, of eliciting significant sexual arousal on the part of the consumers of such materials’. Pornography is distributed through different mediums, including books, magazines, movies, sounds, and animation.

Internet Pornography, or Cyberporn, is the use of the Internet (e.g., porno websites, peer-to-peer file sharing networks, chat rooms, electronic bulletin boards) to distribute pornographic material. The presence of pornographic material on a public and global network such as the Internet raises serious concerns for parents, teachers, institutions, and governments.

The Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly known is widespread. Almost 50% of the websites exhibit pornographic material today. Pornography materials can also be reproduced more quickly and cheaply on new media like hard disks and CD-ROM. The new technology is not merely limited to texts and images but have full motion video clips and movies too. These have serious consequences and have result in serious offences which have universal disapproval like child pornography which

¹³⁹ Shashank Manish: Regulation of Cyber Crime in India, Cri LJ November, 2008- Journal Section, p-308.
¹⁴⁰ Pornography has been derived from two Greek words i.e. ‘porne’ and ‘graphe’. The meaning of word ‘porne is ‘prostitute and word ‘graphe’ is ‘writing’.

{95}
are far easier for offenders to hide and propagate through the medium of
the internet.  

Pornography means polluting through indecent exposure. Cyber
pornography is believed to be one of the largest businesses on the Internet
today. While pornography per se is not illegal in many countries, child
pornography is strictly illegal in most nations today.

Pornography on the net may take various forms. It may include the
hosting of web site containing these prohibited materials, use of
computers for producing these obscene materials, downloading through
the Internet obscene materials. These obscene materials may cause harm
to the mind of adolescent and tend to deprave or corrupt their minds.

**Instances:** A student of the Air Force Bal Bharti School, Delhi,
was arrested in May 2001 for allegedly creating a pornographic website
www.amazing-getns.8m.net. The boy, who was fed up of being teased for
having a pockmarked face, would regularly uphold “morphed”
photographs of teachers and girls from his school into the website. He
was arrested when the father of one of the victims reported the case to the
police.  

**i. Financial Crimes:**

Money is the most common motive behind all crimes including
most of the cybercrimes. Globally it is being observed that more and
more cybercrimes are being committed for financial motive rather than
for “revenge” or for “fun”. With the tremendous increase in the use of
internet and mobile banking, online share trading, dematerialization of

2000.
142 Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters
Kluwer (India) pvt. Ltd. New Delhi, p-168.
shares and securities, this trend is likely to increase unabated. Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams, etc.

Instances: In April 2005, the Pune police arrested five employees of an Emphasis BPO for allegedly stealing almost INR 2 crore from some Citibank customers. The accused had acquired the passwords to customer accounts and then transferred money to accounts opened under fictitious names.143

j. Sale of illegal articles:

It is becoming increasingly common to find cases where sale of illegal articles such as narcotic drugs, weapons, wildlife, etc, is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction website, bulletin boards, etc. It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal article. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button.144

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs, dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as “Internet pharmacies.” These sites offer for sale either approved prescription drug product, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the

143 Ibid. 167.
144 Ibid. 167.
health and safety of patients. The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

**Instances:** In March 2007, the Pune rural police cracked down the illegal rave party and arrested hundreds of illegal drugs users. The social networking site Orkut.com is believed to be one of the modes of communication for gathering people of the illegal “drug” party.\(^{145}\)

**k. Online Gambling:**

It is also called Internet gambling. The habitual and professional gamblers have plenty of opportunities to satisfy their craze for gambling on the internet. There are millions of websites that offer online gambling. They offer online gambling where gamblers upload funds to the online gambling company, makes bets or play the games that it offers, and then cash out any winnings.\(^{146}\) The rapidly growing number of online gambling sites clearly indicates that gambling has become a potential source of entertainment for the computer friendly persons particularly, the youths though they may at times be duped, deceived or cheated by some fake gambling sites.

The special issue with online gambling is that it is legalised in several countries. So, legally the owners of these websites are safe in their home countries. The legal issues arise when a person residing in a foreign country like India (where such websites are illegal) gambles on such a website.\(^{147}\)

---

1. Phishing:

In computing, phishing is a form of social engineering characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit cards, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to a fish for users’ financial information and passwords.

Sending an email to a user falsely claiming to be an established and legitimate enterprise in an attempt to scan the user into surrendering private information they will be used for identity. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, however is bogus and is setup only to steal the users’ information. By spamming large group of people, the phisher counted on the email being read by a brand spoofing or carding, is a variation on, fishing, the idea being that the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into bring it.

With the growing no of reported phishing incidents, additional methods of protection are needed. Attempt includes legislation, user training and technical measures. More recent phishing attempts have started to target the customers of bank and online payment service. While the first such example are sent indiscriminately in the hope of finding a customer of a given bank or service, recent research has shown that phishers may in principle be able to establish what bank a potential


{99}
victim has a relation with, and then sends an appropriate spoofed email to the victim. In general such targeted versions of phishing have been termed as spear phishing.\textsuperscript{151}

**Instances:** An customer of ICICI Bank named Mr. Umashankar Sivasubramaniam lost Rs. 6.46 lakhs through phishing. Mr. Umashankar Sivasubramaniam, who claimed he received an email in September 2007 from ICICI, asking him to reply with his internet banking username and password or else his account would become non-existent. After the reply to this mail he witnessed a transfer of Rs. 6.46 lakh from his account to that of a company which withdraw Rs. 4.6 lakh from an ICICI branch in Mumbai and retained the balance in its account.

On April 12\textsuperscript{th} 2010, the adjudicator of Tamil Nadu, Sri PWC Davidar pronounced a landmark judgement in respect of a complaint lodged with him under ITA 2000 by the award directed the Bank to pay the customer the amount fraudulently transferred in the Phishing transaction along with expenses and interest amounting to a total of Rs 185 lakhs.\textsuperscript{152}

**m. Cyber Defamation:**

Defamation\textsuperscript{153} is defined as “an intentional false communication, either published or publicly spoken, that injure another’s reputation or good name”. Defamation with the advent of computers where certain defamatory information is published or posted through email or chat rooms with an intention to defame the reputation of the person is called cyber defamation. Cyber defamation is not different from conventional

\[\text{References}\]
defamation\textsuperscript{154} except the involvement of a cyberspace medium in the former.

Sending defamatory email, writing derogatory comments on facebook, orkut or other social networking sites also constitutes cyber defamation. The Internet can be used to spread misinformation, just as easily as information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience.

**Instances:** India’s first case of cyber defamation was reported when a company’s employee started sending derogatory, defamatory and obscene e-mails about the Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associate 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 and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.\textsuperscript{155}

**Instances:** Abhishek, a teenaged student was arrested by the Thane police in India following a girl’s complaint about tarnishing her image in social networking site, Orkut. Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile. The profile had been sketched in such way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell

\textsuperscript{154} Section 499 of Indian Penal Code, 1860.

tracked down Abhishek from the false email id that he had created to open up the account.

n. Cyber Stalking:

According to Oxford dictionary, “stalking” is defined as “pursuing stealthily”. Cyber stalking involves following a person’s movements across the internet by posting messages frequented by the victim entering the chat-rooms or constantly bombarding the victim with e-mails etc.

Cyber stalking generally can be defined as the repeated acts of harassment or threatening by the cyber criminal to the victim through the misuse of internet services. Stalking may be followed by serious violent acts such as physical harm to the victim. Many stalkers resort to stalking in order to gain control over their victims. Cyber stalking usually occurs with women who are stalked adult predators or pedophiles.

Cyber stalking is also called as ‘cyber teasing’. Any person who via e-mails or certain messages which are in electronic form, tries to accuse a person or defames his prestige in society is said to be a cyber stalker.

Instances: In April 1999, a 50-year old was convicted in California (USA) for using the Internet to solicit the rape of a woman. He had also terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards. He had posted messages that

---

156 Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters Kluwer (India) pvt. Ltd. New Delhi, p-17

implied that the fantasized about being raped. On at least six occasions, men came to her house saying they wanted to rape her.\textsuperscript{158}

\textbf{o. Web Defacement:}

Website defacement\textsuperscript{159} is usually the substitution of the original home page of a website with another page by a hacker. Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement.

Websites are not only defaced for political reasons; many defacers do it just for the thrill. For example, there are online contests in which hackers are awarded points for defacing the largest number of websites in a specified amount of time. Corporations are also targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general.\textsuperscript{160}

Websites represent the image of a company or organization and these are, therefore, especially vulnerable to defacement. Visitors may lose faith in sites that cannot promise security and become wary of performing online transactions. After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit.

Instances: Mr. Mahesh Mhatre and Mr. Anand Khare were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber

\textsuperscript{158} Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters Kluwer (India) pvt. Ltd. New Delhi, p-17
\textsuperscript{159} In web defacement the original home page of the web is replaced by a pornographic or defamatory page by the hacker.
Crime Cell. They had allegedly used password cracking software to crack the FTP password of the police website. They then replaced the homepage of the website with pornographic content. This act constituted website defacement.\textsuperscript{161}

p. Web Jacking:

Web-jacking is another form of hacking. This term is derived from the term hijacking. In web-jacking, the perpetrator forcefully takes control over the website of another with identical motive of deriving ransom to accomplish is monetary or political purposes. This occurs when someone forcefully takes control of a website by cracking the password and then changing it. The actual owner of the website does not have any control over what appears on that website.\textsuperscript{162}

\textbf{Instances:} In an incident reported in USA, the owner of a hobby website for children received an email informing her that a group of hackers had gained control over her website. They demanded a ransom of one million dollars from her. The owner, a school teacher did not take threat seriously. Three days later she came know from phone calls from across the globe that the hackers had hijacked her websites. Subsequently they had altered the position of the website which was entitled, ‘how to have fun with goldfish’. In all the places where it had been mentioned, they had replaced the word ‘goldfish’ with the word ‘Piranhas’.\textsuperscript{163} Many children believed the content of the website and unfortunately followed

\textsuperscript{161} Prashant Mali: Cyber Law and Cyber Crimes, First Edn. 2012, Snow White publication, p-9
\textsuperscript{162} http://www.asainlaws.org/cyberlaw/library/cc/what_cc.htm.
\textsuperscript{163} Piranhas are tiny but extremely dangerous flesh-eating fish.
the instructions, tried to play with piranhas, which they bought from pet-shops and were very seriously injured.\textsuperscript{164}

q. \textbf{Salami Attacks:}

A salami attack is a series of minor data-security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a Salami Attack.\textsuperscript{165} Crimes involving salami attacks are typically difficult to detect and trace. These attacks are used for commission of financial crimes. These key here is to make the alteration so insignificant that in a single case if would go completely unnoticed. E.g. a bank employee inserts a program into the bank’s servers that deducts a small amount of money (say Rs. 5) a month from the account of every customer.

No account holder will probably notice this unauthorized debit, but the bank employee ill make a sizable amount of money every month.\textsuperscript{166}

This attack is called a “salami attack” because some security specialists claim that it refers to slicing the data thinly, like a salami. Other argues that it means building up a significant object or amount from tiny scraps, like a salami.\textsuperscript{167}

\textbf{Instances:} An employee of a bank in USA was dismissed from his job. Disgruntled at having been mistreated by his employers, he


\textsuperscript{165} Aderucci, Scott. Salami Fraud, www.allnet/CID/attack/papers/Salami.html.


\textsuperscript{167} Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters Kluwer (India) pvt. Ltd. New Delhi, p-175.
introduced a program into the bank system. This program was programmed to take ten cents from all account in the bank and put them into the account of the person whose name was alphabetically the last name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither the account holders nor the bank official noticed the fault. It was brought to their notice when a person by the name of Ziegler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.

From a system development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle.

- **Denial of Service Attack (DOS)**

  This is an act by a criminal who floods the bandwidth of the victim network of fills his email box with spam mail depriving him of the service he is entitled to access or provide. Short for denial-of service attack, a type of service attack on a network which is designed to bring the network down to its knees by flooding it with useless traffic.

  Many Denial of Service attack such as Ping of Death and Teardrop attack, exploit limitation in the TCP/IP protocols. For all

---

168 Mubashshir Sarshar: Cyber Crimes and Effectiveness of Laws in India to control them. Available at http://works.bepress.com/mubashshir/14.
172. A Ping of Death is type of attack on a computer network that involves sending a malformed or otherwise malicious ping. A ping is normally of 64 bytes in size. Sending a ping which is larger than the maximum IP packet size can crash the target computer.
173. A tear drop attack is a DoS attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them.
known DoS attack, there are software fixes that system administrators can install to limit the damage caused by the attack. But, like Virus, new DoS attacks are constantly being dreamed up by hackers. This involves flooding computer resources with more request than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.\textsuperscript{174} Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim computer, exceeding the limit the victim server can support and making the servers crash. Denial-of-service attacks have had an impressive history in the past and have brought down websites like the Amazon, CNN, Yahoo and eBay.

Instances: A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com. In distributed denial of service attacks, the attacker uses zombie’s i.e. computer’s which are unknowingly used by the attacker to simultaneously attacker the target. These zombies’s innocently became the crime abetters.\textsuperscript{175}

s. Privacy Infringement:

Right to privacy is considered as fundamental right in almost all civilized world.\textsuperscript{176} The availability of information in the cyberspace, for anyone with capability to access, has brought up the issue of criminal infringement of privacy. Increasing use of computers and Internet,

\textsuperscript{175} Prashant Mali: Cyber Law and Cyber Crimes, First Edn. 2012, Snow White publication, p-90.
\textsuperscript{176} Mark s. Merkow and James Brietharyst: The E-Privacy Imperative, American Management Association (2002), New York.
people, knowingly or unknowingly store and transmit their personal data, which may be illegally accessed by capable offenders. Under section 72 of the Information Technology Act, 2000, where any person illegally and without consent of the person concerned discloses any electronic book, register, correspondence, information, document or other material to which he got access under any of the provisions of the Act is any rule or regulations made under is liable for breach of confidentiality and privacy.¹⁷⁷

t. **E-mail related crimes:**

E-mail 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 as follows:

i. **E-mail Bombing:** Email bombing refers to sending a large amount of e-mails to the victim resulting in the victim’s email account (in case of an individual) or servers (in case of a company or an email service provider) crashing. Sending numerous or large email messages to one person is considered “e-mail bombing.” Email bombing is characterised by abusers repeatedly sending an email to a particular address at a specific victim site.

E-mail spamming is a variant of bombing: it refers to sending email to hundreds or thousands of users. E-mail spamming can be made

---
worse of the recipients reply to the email, causing all the original addresses to receive the reply.\textsuperscript{178}

Instances: In one case, a foreigner who had been residing in Simla, India for almost 30 years 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 and repeatedly kept sending e-mails till their servers crashed. Foreigner had committed the crime of email bombing on Simla housing board.\textsuperscript{179}

\textbf{ii. E-mail Spoofing}

E-mail spoofing is a term used to describe fraudulent email activity in which the sender’s address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used for spam email and phishing to hide the origin of an email message. By changing certain properties of the email, such as the Form, Return-Path and Reply-To fields, ill intentioned users can make the email appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual well-known website but are run by other party either with fraudulent intentions or as a means of criticism of the organisation activities.

It is forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual code. Distributors of spam often use spoofing in an attempt to get recipient to

\textsuperscript{178} http://www.lse.ac.uk/itservices/help/spamming&spooring.htm, visited at 04/03/12.
open, and possibly respond to such solicitations. Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the email include a sender reporting mistreatment by a spouse to a welfare agency or a “whistle blower” who fears retaliation. However, spoofing anyone other than yourself is illegal in many jurisdictions.\textsuperscript{180} Email spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow a authentication mechanism. Although an SMTP service extension allows as SMTP client to negotiate a security level with a mail server, however this precaution is not an always taken.

If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send message. To send spoofed messages, senders commands in headers that alter the message information. It is possible to send a message that appears form anyone and anywhere, saying whatever the sender wants to say.\textsuperscript{181}

Instance: A branch of the erstwhile Global Trust bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. An investigation revealed that someone had sent out spoofed mails to many of the bank’s customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed email appeared to have originated from the bank itself.\textsuperscript{182}

\textbf{iii. Sending Malicious Codes through e-mails: }E-mails are often the fastest and easiest way to propagate malicious code over the internet.

\begin{flushright}
\textsuperscript{180} Tom Merritt, What is Email Spoofing? www.g4tv.com, visited at 04/03/2012.\textsuperscript{181} \textsuperscript{http://www.mailsbroadcast.com/e-mail.broadcast.faq/46.e-mail.spoofing.htm}, visited at 08/07/2010.\textsuperscript{182} Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters Kluwer (India) pvt. Ltd. New Delhi, p-170.
\end{flushright}
For instance, bug-virus reached millions of computers within 36 hours of its release from the Philippines. Hackers often bind Trojans, viruses, worms and other contaminants with e-greeting cards and then e-mail them to unsuspecting persons. Such codes can also be bound with software that appears to be anti-virus patch.

iv. **Sending threatening e-mails:** This is another way of committing a crime for ransom. With the advance of technology and frequent use of internet, it has become easier for the criminals and gangsters to extract money from the victim by threatening him of his life for any other relative’s life with the help of e-mail by sending it from any part of the world. Any person having a basic knowledge of any part of the world. Any person having a basic knowledge of computer or the use of internet can easily blackmail a person by threatening him via e-mails.

v. **Defamatory e-mails:** E-mails are invariably used to send defamatory libel or slander against the victim in order to compel him to satisfy the lust of the criminal which may be either for money or for satisfying his illegal or unlawful demand or for avenging rivalry.

Defamatory e-mail is extremely fast and simple method of communication by which any kind of messages can be sent to any person throughout the world, in a much more easier and effective manner. When one party makes a false allegation or statement by sending e-mail to another person that can harm that person’s reputation, it is known as e-mail defamation. An e-mail containing the defamatory material must necessarily be published. The publication is complete, sooner a person makes known or delivers the e-mail containing the defamatory matter to another person, other than the person defamed. Thus publishing takes

place merely for forwarding an e-mail to the third person, other than the person defamed.\textsuperscript{184}

vi. **E-mail Frauds:**

E-mail fraud may be defined as any fraudulent behavior connected with computerization by which someone intends to gain financial advantage for himself or for another person, thereby causing economic loss to the victim.\textsuperscript{185}

There are many types of computer frauds and e-mail is a cheaper and popular devise for disturbing fraudulent messages to potential victims. With the development of global communication networks and computers, e-mail frauds are increasingly becoming a global phenomenon. Instance: In 2005, an Indian businessman received an email from the Vice President of a major African bank offering him a lucrative contract in return for a kickback of INR 1 million. The businessman had many telephonic conversations with the sender of the email. He also verified the email address of the “Vice President” from the website of the bank and subsequent transferred the money to the bank account mentioned in email. It later turned out that email was a spoofed one and was actually sent by an Indian based in Nigeria.\textsuperscript{186}

vii. **Harassment via e-mails:**

Harassment through e-mails is not a new concept. It is very similar to harassing through letters. It has become concern for many people. This form of harassment includes directing obscenities towards other, as well as making derogatory comments based for example of gender, race,

---

\textsuperscript{184} Forgery for the purpose of defamation is punishable under Section 469, of IPC.
religion, nationality, and sexual orientation. This type of Internet crime can take place often in chat rooms, through newsgroup, and even through the sending of hate email to targeted mailing lists.

u. **Data Diddling:**

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, or a virus that changes data, or the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved the process of creating recording, encoding, examining, checking, convening or transmitting data.\(^{187}\) This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.\(^{188}\) Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing, the cost can be considerable. To deal with this crime, a company must implement policies and internal controls. This may include performing regular audits, using software with built in features to combat such problems, and supervising employees.\(^{189}\)

Instance: The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council.

---

189. David Bowen, Viruses, Worms and Other Nasties, Protecting yourself online; Department of Interdisciplinary Studies, 2003.
Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who has a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.\(^{190}\)

v. **Internet Time Theft:**

Theft of Internet hours refers to using someone else internet hours. Section 43(h) of the IT Act, 2000 lays down civil liability for this offence. It reads as, whosoever without the permission of the owner or any other person who is in charge a computer system or computer network, charges the service availed of by a person to the account of another person by tampering with or manipulating any computer-computer systems or network is liable to pay damages not exceeding one crore to the person in office.\(^{191}\)

**Instances:** In the Colonel Bajwa case,\(^{192}\) the economic offences wing, IPR section crime branch of Delhi Police registered its first case involving theft of internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd as sent to the residence of the complainant to activate internet connection. However, the accused used Col. Bajwa login name and password from various places causing wrongful loss of 100 hours to him, initially the Police could not believe that time could be stolen. They were not aware of the concept of time theft at all and his report was rejected. He decided to approach the Times of India, New Delhi which in turn carried a report in the inadequacy of the Delhi Police in handling Cyber crimes. The

---

Commissioner of Police, then took the case in his own hands and the Police then registered as case under Section 379, 411, 34 of the IPC and section 25 of the Indian Telegraph Act.\textsuperscript{193}

\textbf{w. Logic Bombs:}

A logic bomb is a programming code, inserted surreptitiously or intentionally and which is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.\textsuperscript{194} Softwares that are inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at the pre-defined time or when some other conditions are met. Many viruses attack their hosts systems on specific days, e.g. Friday the 13\textsuperscript{th} and April fool day logic bombs. A logic bomb when exploded may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.\textsuperscript{195} Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up to date anti-virus program. For best results, the auto-protect and email screening functions should be activated by the user whenever the machines is online. A logic bomb can also be programmed to wait for a certain message from the programmer.

However in some ways a logic bomb is the most civilized programmed threat, because it targeted against a particular victim. The classic use of logic bomb is to ensure the payment is not made by a certain date, the logic bomb gets activated and the software automatically deletes itself.

\textsuperscript{193} Mubashshir Sarshar: Cyber Crimes and Effectiveness of Laws in India to control them. Available at http://works.bepress.com/mubashshir/14.
\textsuperscript{194} M E Kabay, Logic bombs, Part 1, Network World Security Newsletter.
x. **Trafficking:**

Trafficking may assume different forms, it may be trafficking in drugs, in human beings, arms pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.

y. **Computer vandalism:**

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

C. **Jurisdictional Issues in Cyber Law**

As the internet becomes increasingly a medium of commerce. It will become increasingly a medium of fraud. There are many technologies which reduce the opportunity to commit computer related crime. The basic tenets of the opportunity theory are that the level of crime is determined by the availability of suitable targets, the presence of motivated offenders and the absence of capable guardians. The criminal justice administration systems are not equipped to deal with the highly technological crimes committed in cyber world.

It is the judiciary who has the final word on any criminal prosecution and unless the awareness level among them is built up to meet the challenges of increasing cyber crimes. Cyber crimes posses a great challenge before the legislature and law enforcement agencies as there may differences between jurisdictions about whether or not the activity in the question has occurred at all, whether it is criminal, who has
committed it, who should investigate it and who should adjudicate to punish it. These problems can be solved by legislating laws which are more compatible to fit the requirements to regulate the cyber crimes. There should be given a special training of Investigating Officers, Police Officials, Judges and Law Enforcing Agents so that they can understand the meticulous and sophisticated nature of cyber law and then aid for imparting justice to victims.

Jurisdiction is the worst casualty of the technological sphere. Though, jurisdiction, especially the territorial aspect of it, has remained a complex issue in transnational and organized crimes, “those questions are much more common in computer and Internet crimes”. By their very nature, the majority of Internet crimes—whether cyber stalking, unauthorised access, spamming or any other type are done remotely, very often from a different state or country. “While some statutes such as the Computer Fraud and Abuse Act, as shown in United States v. Ivanov explicitly state that they are to be applied extra-territorially, many contain no such provisions and leave the jurisdictional questions for courts to decide”.

1. Traditional principles of jurisdiction

Cybercrimes have extraterritorial aspects. Jurisdiction in relation to State is understood as the terrestrial area within which the sovereign power of the administrator can be exercised. Jurisdiction in relation to a court is the area and the subject regarding which a court has power to take

198 175 F Supp 2d 367 (D Conn 2001).
cognizance and to try a case. Thus, judicial jurisdiction can be defined in following words:

“The scope of the court’s power to examine and determining the acts, interpret and apply laws, make orders and declare judgments. Geographic area, the type of parties who appear, the type of relief that can be sought, and the point to be decided may limit jurisdiction” 201

The concept of judicial jurisdiction of a court emanates from the Sovereignty Theory and Territorial Theory of State. Under this classic formulation, each State is supreme and has unquestionable authority within its geographical limits. Outside a State’s border, was another nation or state with complete authority over its own territory, foreclosing the exercise of jurisdiction by any other State. 202 It was considered as a direct attack on a State’s sovereignty if a judicial process of a foreign State is exercised on its territory. 203 Thus, the territorial paradigm enables a court to readily assert personal jurisdiction over a defendant. 204 In the pre-Internet period, personal jurisdiction was understood in terms of territoriality. 205 The Physical Presence Theory (service within jurisdiction) is one of the core theories on which a court may claim to exercise jurisdiction over a defendant. 206 Both civil and criminal justice systems are governed by the fundamental rule of jurisdiction. So

203 The service of the writ or any other judicial process is the sine qua non of a court’s judicial jurisdiction. The inability of a court to serve a process upon defendant also negates jurisdiction over him. Conversely, if in an action in personam, if service of process is affected then the court can exercise jurisdiction. Thus, basically speaking, the rules as to the legal service of a writ define the limits of a court’s jurisdiction. (A.V. Dicey & Morris, Conflict of laws (13th Edn. Sweet & Maxwell, 2000) 17
204 Supra, n. 30, 26.
205 Ibid.
powerful is the rule that a wrong jurisdiction nullifies the most equitable verdict. At various points of legal history, overlapping jurisdiction in civil and criminal matters are found but they were often successfully resolved by various principles propounded for the purpose. Interaction among different societies, be it on commercial level, contractual level and social level, is as old as the man himself. Criminal link between different communities or countries though on individual level, is also a part of it. This interaction gives rise to several legal complexities when it comes to dispute resolution, settlement of rights or punishing a criminal, as legal provisions of various societies are varied if not opposed to each other.

That was all about the real world, where boundaries are well demarcated and laws are defined and jurisdictional issues are resolved by various principles propounded for the purpose. A court must have jurisdiction and venue so that the dispute is resolved or the accused tried with practical convenience, avoiding unnecessary expense and hardship to the litigants. Jurisdiction is the basic rule of fair play which is essentially two-dimensional in both civil and criminal matters. While in civil matters, it comprises of; subject-matter jurisdiction and personal

208 Venue is the possible or proper place or places for the trial of a suit, as among several places where jurisdiction could be established. Venue established the location where the power of a court should be exercised. It is decided on the basis of convenience and thus, may be waived by the parties. Black’s Law Dictionary (Pocket Edn., 1996) 653.
209 By subject-matter jurisdiction is meant the power of a particular court to hear the type of case that is then before it. Invariably in any country, there would be several courts and tribunals. Like in India, apart from the regular hierarchy, i.e. the Supreme Court, High Courts, District Courts, we also have specialised courts like consumer courts, family courts, income tax tribunals, customs tribunals etc. The IT Act, 2000 has introduced the Cyber Appellate Tribunal (S. 48, Chapter X of the Act). So all these specialised courts, tribunals and authorities have been constituted to determine certain categories of disputes because the law presumes, that for certain kinds of disputes specialisation has to be introduced as such specialised courts and tribunals would be best suited to adjudicate upon a particular kind of complex issue because they have some kind of background in that field. Broadly, a court would only hear a matter that arise within its defined and demarcated area. Raman Mittal, Chap 10 “Dispute resolution in Cyberspace: Determining Jurisdiction and Applicable Law in S. K. Verma & Raman Mittal (Eds.), Legal Dimensions of Cyberspace (Indian Law Institute, 2004) 27
jurisdiction,\textsuperscript{210} in criminal matters, it is personal and territorial, related to the place of commission of crime. As regarding civil jurisdiction, variable rules are found when contractual, consumer, copyright, intellectual property, and trademark disputes are concerned. In such an area, wherever overlapping jurisdictions were manifested in litigations, they were resolved by resorting to theories like choice-of-law rule\textsuperscript{211} and minimum contracts.\textsuperscript{212} Some other approaches include Interest Analysis whereby scholar Brainerd Currie argues that courts would choose what law to apply by looking at the legislative purposes behind each State’s law.\textsuperscript{213}

2. Internet jurisdiction: “\textit{Lex loci delicti}” rule

When one is online, one is almost everywhere. While jurisdiction in erstwhile interpretation-spelled limitation of some sort, be it subject-matter relate or territorial, in the Internet Age it means earthwide. Thus as Street\textsuperscript{214} remarks:

“Court jurisdiction over a party has most often been determined by the presence of the defendant in the state where the court sits. However,

\textsuperscript{210} As the term implies, it is the power of the court to hear or decide a case against an individual personally. It extends the power of the court over persons who fall under its territorial or extraterritorial jurisdiction by way of domicile, residence, citizenship, etc.

\textsuperscript{211} The US Restatement of Conflict of Laws, first promulgated in 1934 created a series of simple, mechanical rules for choosing what law to apply in inter-jurisdictional litigation. The substance of the claim whether the case was based on tort, contract, or property determined the applicable rule. In tort cases, the First Restatement applied a simple choice-of-law rule—\textit{lex loci delicti}, or “the law of the place of the wrong”. Under this rule, a reviewing court would apply the law of the place “where the last event necessary to make an actor liable for an alleged tort takes place”. For contracts, the First Restatement applied a similar formal rule. The law of the place where the contract was made, govern the validity of a contract. The place of making was defined as the place where the “principal even necessary to make a contract” had occurred. Under the First Restatement, real property was govern by the \textit{lex situs}—the law of the physical location. These rules were modified by the Second Restatement in 1971, whereby a rule was laid down, namely, that “when faced with a choice between jurisdictions, courts should apply the law of the jurisdiction with the more significant relationship to the litigation”.


\textsuperscript{213} First, the reviewing court should identify false conflicts. If the choice of one State’s law would advance the policy interests of that State without impairing the policy interests of the State whose law is not chosen, a false conflict exists, and the court should apply the law of the interested State.

\textsuperscript{214} F. Lawrence Street, Mark P. Grant, Law of the Internet (LexisNexis, 2004) 3, 3.01[1].

{120}
courts are now being called upon to adjudicate jurisdictional disputes arising out of the Internet communications in which the parties have little physical or geographic connection with each other or the jurisdiction.”

A website stored on an internet computer server is available for download by anyone around the world through the Internet. E-mail sent through mass “mailing list” transmissions can reach people in many diverse jurisdictions even though the transmitting party did not specifically know or intend that someone from that jurisdiction would become involved.

Uncertainty regarding the proper jurisdiction looms large on the Internet surroundings as the disputable conduct is transmitted through myriad jurisdictions, home and foreign and “it was the decision of the plaintiff to download the information into the forum jurisdiction”.\textsuperscript{215} The consequent results are that the defendant or the accused is faced with such laws which are not applicable on him; in fact the resultant local bias is all what the defendant is made to face.\textsuperscript{216} Courts all around the world are showing an assertive attitude to extend their powers beyond physical boundaries in order to help local parties.

For example, an English court in the Queen’s Bench Division of the Royal Court of Justice in London allowed a plaintiff to effect service of process in an attempt to enjoin threats that had been delivered by e-mail over the Internet when the service of process was to be delivered through e-mail. Current court service of process rules allowed service via

\textsuperscript{215} Ibid, 3-4, 3.01[1].
\textsuperscript{216} An Australian court has recently ruled that an Australian citizen may sue Dow Jones & Co., publisher of the Wall Street Journal, for defamation under Australia’s strict defamation laws. The article that allegedly defamed the Australian citizen appeared on the online version of the newspaper,\texttt{<http://www.nando.net/technology/story/85536p-1145746c.html>} (2001).
personal service, regular mail, and fax or “in such manner as the court may direct”.

As a single act on the Net is the work play of several participants, as there are website owners, the online intermediaries, the host, the author or creator of a piece of writing or painter, etc., the corporate, the end-user and so on. Hence a single infraction or wrong may involve all or some of these and again as the nature of the Net goes, it is quite possible that all of these come from various countries and hence, from various jurisdictions. In such a case, even if one applies the traditional principles of jurisdiction, some of these may fall in different jurisdiction by virtue of subject-matter jurisdiction and some may fall yet another jurisdiction due to personal jurisdiction and yet some of the participants may remain uncovered by these principles. This leads to the birth of a law of cyberspace based on private contracting on a global basis and enforced by a combination of the sysop’s (system operators) ultimate right to banish unruly users and the user’s ultimate right to migrate to other online service providers (such as ISPs). The hazy scenario calls for several suggestions from various thinkers as some of them are of the opinion that the traditional principles are inapplicable to such situations and altogether a new catena of jurisdictional rules are required for the cyberspace. Traditional theories of jurisdiction are inapplicable to the Internet due to the following reasons:

1. Material posted on the Internet has worldwide audience;
2. It is easy to move a website from one territory to another;

217 Ibid, 3-6, 3.01[3].
220 Supra, n. 30, 44.

{122}
3. A website can be hosted on one area, but directed at users in another geographic location;
4. Parts of a website may be hosted in one area, while other parts of the website are hosted in another location; and
5. It is not always possible to determine where a website or user is located.

All this calls for the application of new rules regarding Internet jurisdiction.

3. **Areas of conflict: Traditional notions of jurisdiction and the Internet**

   Moreover, the advent of Internet overturned the century-old established theories of jurisdiction which were deeply rooted in the territorial and physical concept. While the Internet absolutely negate tangibility and terrestrial forms; applicability of laws of the physical world are bound to face unprecedented legal hardships. The main areas of conflict are discussed in the subsequent sections.\(^{221}\)

   a. **Inter-sovereign conflict**

   Extension of laws of one State to another has been an unimaginable concept unless it is backed by some treaty between the two States. For the Internet environment, this is the first requirement as the borderless world knows no such established norms. The conflict thus arises.

   b. **Over-inclusiveness**

   Most of the traditional theories of jurisdiction are over-inclusive in relation to the Internet because they allow for the almost unlimited exercise of judicial jurisdiction.\(^{222}\) The traditional view rests on the concept that every sovereign State hast unquestionable authority within its geographical limits but when a website is created, the server is

---

\(^{221}\) Ibid.
physically located within the boundaries of the State concerned. While such State, as according to traditional notions, has legitimate control over its subjects and over the physical infrastructure of the Internet (server, etc.), the particular Web page being visible in any part of the globe, all the 300 States of the planet may have; applying the same traditional notions, equal authority and interest. Recognising the equal rights of all the States, there is witnessed a conundrum of jurisdictional powers; the over-inclusiveness.

c. **Under-inclusiveness**

Another dimension in one of the traditional theories is that it advocates the limits of a State’s authority within its territorial boundaries. It shuns the idea of crossing these boundaries. In the Internet surroundings, if a dispute arises (which is happening daily) where the plaintiff and defendant are from two different jurisdictions then the concerned States are forbidden to cross the limits. Thus, the under-inclusiveness of traditional concepts is revealed because of the States that want to regulate Internet activities cannot effectively enforce their laws against “purveyors of harmful material through the Internet” who are located outside their territorial borders.223

**D. Regulation of Cyberspace**

a. **Need for regulation of cyberspace activities**

A good starting point for an illuminated argumentation on the criminalisation of activities in cyberspace is the aspect of regulation of these activities itself and associated questions of its desirability, necessity and feasibility. The rhetoric of the cyber libertarians, seeking self-regulation of the internet, while challenging perceived essentialities for

223 Ibid.
any kind of regulation, like territorial boundaries, real relationships and notions of property, is firmly grounded on the assertion that cyberspace is capable of being regulated through the creation of institutions and mechanisms for the regulation of conduct in cyberspace through the formulation of community based rules that are constituted, decreed and enforced by its participants without necessitating state intervention. On the other hand, those demanding government regulation stress on the inadequacy of such a system to combat instances of grievous criminality.

A closer look at the contentions of both parties provides an academic space for a discussion on the criminalisation of cyberspace activities and a canvas to contextualise the nature of offences introduced by the amendment.224

The cornerstone of the self-regulation theory is that the absence of government involvement in regulatory mechanisms does not result in cyberanarchy and suggests that the application of geographically based conceptions of legal regulation to cyberspace activities makes no sense at all, and further, that cyberspace participants are better positioned than the government to design a comprehensive set of rules that are cheaper to enforce and are practically sound.225 The justification for such an idealistic viewpoint is buttressed by moral considerations often expressed by the participants of cyberspace who unequivocally express their objections to being disciplined by orders of the government and declare the space that they have created for themselves to be independent of the tyrannies of government order.226

Entrusting the internet community with the power to create legal rules and institutions will overcome inherent difficulties associated with geographical determinacy and territorial enforcement and evolve into a mechanism to govern a wide range of new phenomena that have no clear parallel in the non-virtual world,\textsuperscript{227} thus saving the legislature the time and energy to draft laws to deal with such situations. The proponents of self-regulation draw credibility from their claim that State laws enacted to deal with cyberspace activities have been unsuccessful,\textsuperscript{228} and that existing laws and methods of lawmaking are inadequate,\textsuperscript{229} and so, the internet should be self-regulated. The underlying principle entrenched in these views is that cyberspace is the antithesis of regulations and the impracticalities of regulation by external forces including law enforcement forces are too compelling to make such an attempt. The dispensability of government intervention is intimately twined with the complicated nature of social relationships in cyberspace, wherein criminal acts are reprimanded by third party Internet users who impose community defined sanctions on offenders as a form of punishment akin to State law enforcement mechanisms that seek to penalise the same crimes by utilizing additional State resources with less than desired effects.

b. Need for criminalisation of offences in cyberspace:

To highlight the limitations of self-regulation, or the opposite parties’ contentions in this case, would be to make a case for the criminalisation of offences in cyberspace through State intervention, a

\begin{footnotesize}
\begin{itemize}
\end{itemize}
\end{footnotesize}
position several scholars have taken with the advent of serious offences and increasing criminality on the internet such as paedophilia, cyber frauds, data theft, impersonation and cyber terrorism.\textsuperscript{230} The typical self-regulation punishment model is centred on banishment from the group,\textsuperscript{231} a procedure for social control that appears lenient and lacking in deterrence value as opposed to criminal sanctions imposed by the State to deter any destructive or anti-social conduct in cyberspace. It appears that the stream of anti-governmentalism has been laid to rest in view of the fact that the internet has quite simply become too mainstream, and being the preferred platform for electronic commerce, the need for governmental regulation cannot be ignored.\textsuperscript{232} Perhaps the greatest argument in favour of criminalizing unlawful conduct on the internet is its distinctiveness from territorial crime.

The very fact that cyber crimes are easier to learn how to commit, require fewer resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present in it and the fact that they are often not clearly illegal\textsuperscript{233} make criminalisation of such conduct not only important, but essential. The conclusion that must be reached is that the State must step in with some level of regulation of cyberspace.\textsuperscript{234}

\textsuperscript{231} Based on terms and conditions of access and use, imposed by service providers, commonly referred to as ‘netiquette’.\textsuperscript{2011} 107.
c. Types of offences to be criminalized:

An analysis of the new crimes introduced by the IT (Amendment) Act on the touchstone of cyberspace conduct sought to be criminalised by statutes and conventions around the world would help in determining the suitability and stringency of the new sections in the Indian scenario.

There are essentially four main types of conduct that a domestic legislation should penalise –

1. offences against the confidentiality, integrity and availability of computer data and systems,
2. computer-related offences with the intention to defraud,
3. content related offences, and
4. offences related to infringements of copyright and related rights.

In order to acquire a jurisprudential understanding of cyber crimes in general, and to gain a critical insight into the nature of offences introduced by the amendment and whether they serve the function expected of them, it is important to comprehend why these particular forms of conduct are criminalised across jurisdictions. Further, it is also essential to understand the range of unlawful conduct that involves computers. With the first, second and fourth type of conduct, private individuals may not be able to detect and proceed against the perpetrators and it therefore falls upon the State to intervene and impose criminal sanctions. It is necessary to criminalise acts falling within the third category as they are offences that shock the conscience of society and threaten public morality.

Conclusion:

Cyber crime is extremely efficient i.e. it operates and affects within no time, it may take seconds or a few minutes to hack websites or play Cyber frauds. Cyber crime knows no geographical limitations, boundaries or distances. A cyber criminal on the moon can hack computers in Delhi or play Cyber Frauds by transferring Funds from the bank in New York to his account in Sydney.

Cyber Crime has the potential of causing and injury which is unimaginable magnitude. It can easily destroy web-sites created and maintained with huge investment or hack into confidential zones such as defense system of a country or do scam of a magnitude which can shake economics correspondingly, cyber crime is very profitable to commit. Cyber Crimes are easy to commit and the weapons to commit the same are easily and freely available in CDs and even on the Internet. The act of Cyber Crime takes place in Cyber space which makes the cyber criminals almost invisible.

A Cyber Criminal is here, there, nowhere, anywhere and everywhere. Therefore the degree of risk in cyber criminality is extremely low in comparison to other traditional crimes such as murder rape and kidnapping.236

***

236. Vivek Sood, Cyber Law at p. 72