A. **INTRODUCTION**

The offences which take place on or using the medium of Internet are known as cybercrimes. These include a plethora of illegal activities. The term ‘cybercrime’ is an umbrella term under which many illegal activities may be grouped together. Because of the anonymous nature of Internet, there are many disturbing activities occurring in the cyberspace which may enable the perpetrators to indulge in various types of criminal activities which are called as cyber crimes.

The weapon with which cybercrimes are committed is technology and therefore, the perpetrators of these crimes are mostly technically skilled persons who have a thorough understanding of the Internet and computer applications. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber-pornography, cyber-defamation etc. Some conventional crimes may also be cybercrimes if they are committed through the medium of Internet. For e.g theft, fraud, cheating, mischief, misrepresentation, intimidation etc. which are all punishable under the IPC, 1860.

Thus, cybercrime means any unlawful act wherein the computer is either a tool\(^1\), or a target\(^2\) or both.

B. **MEANING AND DEFINITION OF CYBER CRIME**

1. **Information Technology Act 2000**

   As regards exact definition of cybercrimes, it has not been statutorily defined in any statute or law as yet. Even the IT Act, 2000 does not contain the definition of cybercrime. However, cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus, any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime.

2. **Prof. S.T. Viswanathan**

   He has given 3 possible definitions of cyber crimes and these are as follows:

   a. Any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

   1. Cybercrimes which involve computer as a tool are usually modification of conventional crimes such as drug-trafficking, on-line gambling, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyber-stalking, spoofing etc.
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 transmission of data.  

3. **UN Congress on Prevention of Cyber Crime and Treatment of Offenders**

Cybercrime as defined internationally by the UN Congress on Prevention of Cyber Crime and Treatment of Offenders\(^4\) comprises of following 2 categories:

i. **Narrow sense:** cybercrimes in a narrow sense connotes a computer crime and includes any illegal behavior directed by means of electronic operations that targets the security of the computer systems and the data processed by them.

ii. **Broader sense:** cybercrime in broader sense includes all computer related crimes and consists of any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

C. **NATURE OF CYBER CRIME**

The term ‘cyber’ is derived from the word ‘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, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.

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

Though there is nothing new in the adoption of new technologies by criminals. In the era of liberalization and globalization we must recognize cyber crime as significantly new

---


4 Tenth UN Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.
phenomenon which has political, social and economic impact worldwide. Cyber crime is a threat to national and international socio-economic, political and security system.\(^5\)

D. **SCOPE OF CYBER CRIME**

Presently, cyber crime is an ever increasing phenomenon, not only in India but all over the world. The incidence of cyber crime is directly proportional to the level of progress made by a country in computer technology. The report of the United Nations\(^6\) stated that more than 50% of the websites in the US, Canada and European countries have experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies. A new trend that has developed in recent years is that the militants are going for terror training. The Internet has become a key teaching tool for militants who are using it to educate recruits in cyber terrorist’s training camps.

Gabriel Weimann, an Internet and security expert who teaches in the University of Mainz in Germany and has studied militant’s use of website for nearly a decade, while addressing the Internet security personnel said that, “website and chat room used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda but also for terrorist education. Al-Qaida has launched a practical website that shows how to use weapons, how to carry out kidnapping and how to use fertilizers to make a bomb.”\(^7\)

The computer related crime has already become an area of serious concern for most of the countries of the world, and India is no exception to it. The prime factor that has to be taken into consideration while deciding whether a particular computer related activity be reckoned as cyber crime is that a distinction must be drawn between what is unethical and what is illegal. It is only when an activity is truly illegal, it should be treated as crime and the prosecution of the offender must be sought. Therefore, criminal law should be implemented with restraint in determination of cases which relate to cyber law.\(^8\)

In the absence of an internationally recognized definition of cybercrime or computer crime, there has been a great deal of debate amongst the legal experts on the term ‘computer misuse’ and ‘computer abuse’, which are frequently used in the context of cyber crime. However, the practice in vogue in this regard is to hold that the 2 terms have different

---


\(^7\) Gabriel Weimann was addressing a Conference on Internet Security at the headquarters of Germany’s Federal Police Office, as reported in the *Times of India*, Delhi edition, dated November 23, 2007.

implications. The criminal law applicable to cybercrime must make a distinction between incidental misuse of a computer system, negligent misuse and intentional misuse of computer system and it is the later, which should be treated as a crime and not the former two. As a corollary of this distinction, it is the abuse of a computer system which should be treated as criminal behavior punishable under law and not the behavior which causes annoyance or discomfort to the computer user.

E. CHARACTERISTICS OF CYBER CRIME

As a result of development of technology, a new variety of crime called the cyber crime has emerged which is radically different from the traditional crimes. This crime is the ill-effect of the development of Internet regime. In view of the peculiar nature and repercussions of cybercrime, its characteristics are altogether different from that of a conventional crime. Following are the main characteristics of cybercrime:

1. **Low risk high rewarding ventures**
   
   The most striking feature of cybercrime is that they are relatively easy to commit, difficult to detect and even harder to prove. The cyber criminals with basic computer knowledge and skill can easily destroy valuable database causing huge loss or damage to the affected victims of the crime.  

2. **Lack of awareness among victims**
   
   Many a times, the victim affected by cybercrime is unaware of its occurrence because of lack of adequate skill and know-how in handling the computer system.

3. **Physical presence not required**
   
   The cybercrime can be committed even from a far distant place without the necessity of its perpetrator’s physical presence at the scene of crime.

4. **Lack of hi-tech skills among investigating agencies**
   
   The detection of cybercrimes requires hi-tech skill which the investigators generally lack.

5. **Victims refrain from reporting cases**
   
   More often than not, the party or the organization victimized by the cybercrime prefers to refrain from reporting it to the police for the fear of adverse publicity or possibility of the loss of public trust in them. The reluctance of the victims to come forward and file a

---

9 S.K. Bansal, Cyber Crime, 2003, p.17
police complaint further aggravates the magnitude of the problem of cybercrime detection and control.

6. **No violence is involved**
   
The cybercrime does not involve any violence, but is rather an outcome of greed, mischief and exploiting the weakness of the victim.

7. **No territorial boundaries**
   
The problem of cybercrime becomes more complex because Internet knows no territorial boundaries, which enables the criminal to remain out of reach of law in most of the cases.

8. **Anonymity and Openness**
   
The computer network used for information dissemination has the feature of anonymity and openness which make it easy and convenient for the criminal to indulge in crime without being identified or known to the computer user who is a victim of his illegal activity.\(^{11}\)

9. **Paucity of authentic evidence**
   
   Since all information over a network system is exchanged in the form of electronic data, there remains no trace of data once it is erased and the destruction of this sole evidence enables the criminal to remain undetected and escape criminal prosecution.

10. **Have wider ramifications**
    
The range of cybercrime is wider enough to affect the socio-economic as also the legal rights of the people.\(^{12}\)

**F. ELEMENTS OF CYBER CRIME AND CRIMINAL LIABILITY**

   Generally there are 2 elements of crime namely, mens rea and actus reus with certain exceptions. For e.g. in conspiracy only mens rea is enough for imposing criminal liability whereas in crimes against state like false evidence, counterfeiting coin, white collar crime etc. only actus reus is sufficient to impose criminal liability. The general principle of criminal law is that no person is to be convicted of a crime unless it is proved beyond reasonable doubt by the prosecution that his conduct (act or omission) is prohibited by criminal law and he is

---

\(^{11}\) “When Private becomes Public in Cyberspace”, *The Tribune*, March 17, 2008, p. 19

\(^{12}\) Ashish Pande, *Deviation and Prevention*, 2006, p. 126
liable for the same and also that he had a defined state of mind in relation to the crime commission. Thus, actus reus unaccompanied with mens rea is not a crime.

Actus reus + Mens rea = Crime
Actus reus + No Mens rea = No Crime
No Actus reus + Mens rea = No Crime

J.C. Smith and B. Hogan considered actus reus as such result of human conduct as the law seeks to prevent. In the case of cyber crime, it is very difficult to prove both elements of crime.

1. Actus reus

The actus reus of cyber crime is very dynamic and varied. For e.g. when with a keyboard and mouse one start functioning with computer, when one is attempting access to information on other’s computer without the consent or approval of the authorized person, when is one attempting for hacking, flowing viruses, to commit cyber crime and actually caused those acts etc. these are human conduct or actus reus in cyberspace which law seeks to prevent i.e. they are actus reus of cyber crimes.

2. Mens rea

Mens rea is another essential element of cyber crime. According to Smith and Hogan, till 12th century, only for actus reus a person could be held liable for any injury without proof of mens rea or blameworthy state of mind. In modern Common Law this concept has been changed and now guilty mind is the essential element for crime commission and imposition of penalty. The term ‘mens rea’ is not used and defined in the Indian Penal Code, 1860. However, the use of words like fraudulently, dishonestly, knowingly, recklessly, intention etc. represents mens rea. For e.g while committing hacking, the hackers have knowledge or intention of unauthorized access and thereby commission of cyber crime.

G. FACTORS RESPONSIBLE FOR CYBER CRIMES

Professor H.L.A. Hart in his classic work entitled ‘The Concept of Law’ has stated that human beings are vulnerable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Applying the same analogy to cyberspace, the computer systems despite being hi-tech devices, are extremely vulnerable. This technology can easily be used to dupe or exploit a person or his computer by illegal or

---

unauthorized access. The damage so caused to the victim may be direct or indirect result of abuse of computer systems. In the absence of any foolproof mechanism to protect and safeguard innocent computer users against cyber criminality, the cyber criminals indulge in criminal activities through networks unabated without any fear of being apprehended and tried for the offence committed by them.

The reasons for vulnerability of computers to cyber criminality may briefly be stated as follows:

1. **Huge data storage capacity**
   The computer has a unique characteristic of capacity to store huge data in a relatively small space. A small micro-processor computer chip can store lakhs of pages in a CD-ROM. This storage capacity\(^\text{15}\) has enough space to remove or derive information either through physical or visual medium in a much easier way. Any data stored in ROM\(^\text{16}\) 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 over-written.

2. **Wider access to information**
   Computer is an electronic device which carries out its functions with the help of complex technology rather than manual actions of human beings. The greatest advantage of networking in the computer age is the wider access to information resources over a large and extensive medium. More and more organizations are resorting to networks for providing easily accessible information to their employers, customers and parties with which they deal. This is the reason why networking and cyber activities are increasingly becoming the order of the day in the present information age.

   Information dissemination through World Wide Web\(^\text{17}\) has created new resources for faster and cost effective easy access to information throughout the world. It has created new environment of e-mails, chats, downloads etc. Now each and everyone is just a mouse\(^\text{18}\) click away from another. However, wider access to information creates some problems like protecting and guarding any computer system against unauthorized access where there is

---

\(^{15}\) The storage capacity is measured in terms of ‘bytes’, ‘megabytes’ and ‘kilobytes’. Kilo stands for 1000 and one mega byte equals to about 500 pages of the text.

\(^{16}\) ROM stands for ‘Read Only Memory’. It is a type of memory that can hold data permanently or semi-permanently.

\(^{17}\) www is a network of sites that can be searched and retrieved by a special protocol known as Hypertext Transfer Protocol (http). Mere writing of address automatically reaches the internet and brings the sought information on the screen.

\(^{18}\) In the context of computer, ‘mouse’ is a printing device that functions by detecting two dimensional motions relating to its supporting surface.
possibility of breach, not due to human error, but because of the complex technological manipulations.

3. **Complexity of computer systems**

   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 possible that there might be a lapse at any stage. The cyber criminal take undue advantage of these lapses and lacunae and penetrate into the computer system. Such criminals are called hackers who exploit the weaknesses in existing operating systems and security devices. Thus, hackers are the dreaded enemy of the Internet and general network security and they exploit the complexity of computer systems motivated by personal vengeance, sabotage, fraud, greed or malice against the victim.

4. **Negligence of network users**

   Negligence is closely related to human conduct. Therefore, it is quite probable that while protecting the computer system there might be any lapse or negligence on the part of user which may provide an opportunity for the cyber criminal to gain unauthorized or illegal access or control over the computers. Interaction with the cross section of computer users has shown that in their anxiety to put the computer software into regular operation, they allow the access, control and security measures to take a back seat, thus providing scope for cyber criminals to intrude and steal, alter or erase substantial data. This is particularly true with big organizations such as banks, corporations, Government offices etc. which are equipped with hi-tech software systems for public access but leave it totally insecure and unguarded against information poachers or manipulators due to sheer negligence of their staff or employees.  

5. **Non-availability or loss of evidence**

   The traditional methods for producing, storing, transmitting and disseminating information or records has now been replaced by the digital computer processing and network technology. The real issue before the law enforcement and investigating agencies is how to procure and preserve evidence. Unlike traditional offences, it is very difficult to collect sufficient evidence of a cyber crime which could withstand judicial scrutiny to establish the guilt of the cyber accused beyond doubt. Anonymity, which Internet provides to the cyber criminals, encourages him to indulge in criminal activity without leaving any evidence and even if some evidence is left, it is hardly sufficient to convince the police that a

---

criminal case can be registered against the perpetrator. The poor rate of cyber conviction is a pointer to the fact that most cyber criminals destroy evidence in order to escape conviction.

The inadequacy of traditional methods of evidence and crime investigation has necessitated adoption of new techno-legal procedure called cyber forensics. The forensic experts play an important role in collecting and presenting admissible electronic evidence and search and seizure of material evidence relevant to the cyber crime under investigation, but still there are certain grey areas which enable the cyber criminal to tamper with the evidence to mislead the investigating agencies.\(^\text{20}\)

6. **Jurisdictional uncertainty**

Cybercrimes cut across territorial borders which undermine the feasibility and legitimacy of applying domestic laws which are normally based on geographic or territorial jurisdiction. Cybercrimes are committed through cyberspace network interconnectivity and therefore, they do not recognize geographical limitations because of their transnational in nature. There being no uniformity in law and procedure among the different nations for handling cyber criminals, jurisdictional conflict poses a serious threat for a nation to deal with the cyber offenders. In many cases, it so happens that a particular cyber activity is recognized as a crime in one country but it is not so in the country in which the criminal or the victim resides, with the result the criminal easily escapes prosecution. In the absence of a single internationally recognized code of law and procedure governing cyber crimes, the law enforcing authorities of the individual countries find it extremely difficult to tackle cybercrimes and criminals applying their territorial law. Thus, reporting and conviction in cyber cases is far and few due to paucity of cyber jurisdiction of the country investigating these offences and this uncertainty of law encourages the cyber criminals to continue their nefarious activities unabated.

Recently, the IT security firm McAfee reveals a global investigation of targeted intrusions or cyber attacks on governments, corporations and non-profits. The investigation, dubbed ‘Operation Shady RAT’- a commonly used acronym for remote access tools that allow you to access computers from a remote location- tracks a series of cyber attacks on 72 organizations across 14 geographic locations, over a period of 5 years. Ever since the 14-page report went viral on the Web, speculation is rife about the source of attack. The report itself does not mention the perpetrator, though it observes that the fact that the Asian and Western

National Olympic Committees, IOC and the World Anti-Doping Agency have been hacked into points to a non-commercial motive to these attacks. The report alludes to possible involvement of ‘a state actor’. As for as the modus operandi of these attacks is concerned, the attacks were simple in procedure, executed by sending a spear-phishing email containing an ‘exploit’ which, when opened, automatically downloads malware on to the computer’s hard-disk. This malware — a set of instructions on your computer— will set up a new communication channel to the ‘command and control’ Web server. Dmitri Alperovitch, author of this report and Vice-president of Threat Research at McAfee, said that “after painstaking analysis of the logs, even we were surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators.”

Table: McAfee Global Investigation of Cyber Attacks

<table>
<thead>
<tr>
<th>Victim’s Country of Origin</th>
<th>Victim Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>49</td>
</tr>
<tr>
<td>Canada</td>
<td>4</td>
</tr>
<tr>
<td>South Korea</td>
<td>3</td>
</tr>
<tr>
<td>Taiwan</td>
<td>3</td>
</tr>
<tr>
<td>Japan</td>
<td>2</td>
</tr>
<tr>
<td>Switzerland</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2</td>
</tr>
<tr>
<td>Indonesia</td>
<td>1</td>
</tr>
<tr>
<td>Vietnam</td>
<td>1</td>
</tr>
<tr>
<td>Denmark</td>
<td>1</td>
</tr>
<tr>
<td>Singapore</td>
<td>1</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>1</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
</tr>
<tr>
<td>India</td>
<td>1</td>
</tr>
</tbody>
</table>

Though the McAfee’s report only said that a ‘State-actor’ could be behind the hacking, but from the timing of the attack and the nature of its targets, several security

---

21 “State actor linked to major cyber intrusions in India, World: McAfee report says 72 organizations in 14 countries hacked into for years”, The Hindu, August 4, 2011, p. 1

22 Ibid, For details see www.mcafee.com as visited on August 5, 2011
experts had pointed a finger at China. Days after being linked to a massive global hacking campaign, China had blamed India and the US for targeting it in thousands of cyber attacks over the past year. The National Computer Network Emergency Response Coordination Centre, which is the Chinese government’s ‘primary computer security monitoring network’, recently released an official report claiming that about half of 4,93,000 cyber attacks on the websites of Chinese government and other agencies ‘originated from abroad, particularly the US and India.’ It said that the attacks were in the form of malicious ‘Trojans’ software, with 14.7 per cent linked to Internet Protocol addresses (IPs) in the US and 8 per cent in India.  

H. CLASSIFICATION OF CYBER CRIME

Cyber crimes are classified into various types on the following basis:

1. Based on Old or New Crimes Committed on Computers

Whether an old crime is committed on or through computer or a new crime is committed, cyber crimes are of following 3 types:

   i. Crimes ‘on’ the Internet

   These are the old crimes which are committed on or through the new medium of the internet. For e.g. cheating, fraud, misappropriation, defamation, threats etc. committed on or through or with the help of the internet. The internet with its speed and global access has made these crimes much easier, efficient, risk-free, cheap and profitable to commit.

   ii. Crimes ‘of’ the Internet

   These are new crimes created with the internet itself, such as hacking, planting viruses and IPR thefts.

   iii. New crimes used for commission of old crimes

   For e.g. where hacking is committed to carry out cyber fraud.

2. Based on the Victim of Cyber Crimes

Depending upon the victim of cyber crime, it may be broadly classified under the following 3 heads:

   i. Against Individuals

   Under this category it can be against individuals or against individual property through the means of:

---

a. Harassment via e-mail
b. Cyber stalking
c. Dissemination of obscene material
d. Defamation
e. Unauthorized control/access over computer system
f. Indecent exposure
g. E-mail spoofing
h. Cheating and fraud
i. Computer vandalism
j. Transmitting virus
k. Net trespass
l. Intellectual property crimes
m. Internet time thefts

ii. Against organizations
Against organizations, cyber crimes can be through the means of:

a. Unauthorized control/access over computer system
b. Possession of unauthorized information
c. Cyber terrorism against government organization
d. Distribution of pirated software etc.

iii. Against society at large

a. Pornography
b. Indecent exposure
c. Trafficking
d. Financial crimes
e. Sale of illegal articles
f. Online gambling
g. Forgery

3. Based on Nature of Cyber Crime
Based on nature, the cyber crimes are divided into following 2 heads:

i. Social cyber crime
The main social cyber crimes are:

a. Trafficking
b. Cyber obscenity & pornography

c. Cyber terrorism

d. Cyber fraud

e. Cyber gambling
ii. Economic cyber crimes

Economic offences affecting more than $1.2 trillion e-commerce industry worldwide includes the following:

a. Credit card schemes
b. System corruption
c. Internet fraud
d. Dot com job scams
e. Corporate and political espionage
f. Mafia and drug peddlers
g. Multi site gambling websites

4. Based on the Role of Computers

Depending upon the role played by computer in perpetrating crime, the computer may be involved as a victim of crime, or as an instrument used to commit a crime, or as a repository of evidence related to the crime as is discussed under the following 3 heads:

i. Computer as a ‘victim’ of crime

A computer or a computer network could be the target of an offence wherein the computer becomes the victim. In such cases, the computer’s confidentiality, integrity, or accessibility is attacked. The information stored or the service provided by the victim is stolen or the victim is crippled and damaged. Such crimes involve disrupting the functioning of the computer, computer system or computer network; corrupt the operating systems and programmes; theft or disturb data or information; intellectual property violations and blackmail using personal information hacked from computer systems. Example of this form of computer crime is the denial of service attacks on popular internet sites like Yahoo, CNN etc. and the spread of the ‘Melissa’ and ‘I Love You’ viruses and their variants.

ii. Computer as a ‘tool’ of crime

Computer can be used as a tool or an active weapon for committing a crime which includes frauds, IPR violations, online transactions of illegal goods etc. computers can also be used as any other hi-tech equipment for committing traditional crimes. Such crimes include automated teller machine (ATM) frauds, credit card frauds, frauds involving electronic fund transfer (EFT), embezzlement of funds from the banks, telecommunication frauds, counterfeiting and software piracy. These are also
called as computer assisted crimes. When the computer is used as an active weapon for perpetuating the crime, it is also termed as ‘information crime’, as it could not be committed in the absence of information technology.

iii. **Computer as a ‘witness’ to crime**

A computer need not be only a victim or a tool; it could also be the witness to the offence. The examples of computer as a witness to crime is the money laundering, illegal banking transactions, bulletin board system (BBS), storage of drug trafficking transaction records (viz. the purulia arms drop case, wherein the details of money transactions were stored in a laptop computer). Further a computer system may be used to detect information, which assists the criminal in commissioning the crime. For e.g. an employee of Barclays Bank in the USA used the bank’s computer to discover a dormant account, forged the account holder’s signature and withdrew $ 2,100. In such cases the computer is incidental to other crimes.

5. **Based on Nature, Source, Motive and Impact of Cyber Crime**

Depending upon the source, nature, motive and the impact, crimes can be of following 3 types:

i. **Computer crimes**

Computer misuse is a crime committed against a computer system or other digital media. It includes digital crimes such as computer hacking, illegal access, use of backdoors, viruses and other unauthorized intrusion or abuse.

ii. **Computer related crimes**

Such crimes include computer pornography, theft of intellectual property and software copyright etc.

iii. **Network crimes**

The computer network crime or the computer aided crimes are those where a computer or other digital media is used to facilitate crimes, such as blackmail, where the demand is sent via internet and such crimes are committed against e-commerce suppliers.

6. **Based on the Criminal Activities**

Depending upon the criminal activities, computer crimes are of following 3 types:

i. **Physical crimes**
The physical crimes are related to computer or its associated peripherals, hardware, software or the computer time. For e.g. theft, breakage, destroying the data, output or media and inter-processing manipulations.

ii. Data related crimes
In the data-related crimes, unauthorized data or information in the digital form is entered in the computer systems or the data that should be entered is altered, suppressed or corrupted by the criminals so as to gain undue advantage. Computer fraud by input manipulation is the most common computer crime, which is easy to perpetrate and difficult to detect. The data-related crimes could further be sub-classified into the following 4 categories:

a. Data diddling
It is the most common form of computer crime, which is carried out by input manipulations. It involves changing the data, with malicious intentions, during or before feeding it into a computer and provides undue advantage to a specific party. It also includes adding fraudulent input data, altering the input data, omitting the desired input data, wrongly posting a transaction, making alterations or additions in the master file records, posting the transactions partially, destroying the output, and substituting the counterfeit output. Such types of changes can be affected by anyone associated with the process of creating, recording, encoding, examining, checking, converting and transporting data that enters a computer.

b. Data leakage
It involves illegally copying the master file information of the computer for ransom, blackmailing or any other fraudulent purposes.

c. Data spying
For spying on the sensitive information of a person, his computer network is assessed from a remotely located computer, by using the legitimate password, or breaking the password. Such data is sold to others at a very high price.

d. Scavenging
It is a method of obtaining or re-using the information, which might have been left after processing, in or around a computer system.

iii. Software-related crimes
In such crimes, the system as well as the application software are affected or corrupted. As this is very sophisticated form of crime and is much more dangerous so it is difficult to detect. Further it involves changing existing programmes in the computer system or inserting new programmes or routines and the computer programmers, analysts and other experts are involved in commissioning or making alterations in the software. The software-related crime could be perpetrated by using various techniques like computer viruses, computer worms, Trojan horse, trap door, super zapping, wire-trapping, time bombs, logic bombs, and salami attacks etc.

I. SOME IMPORTANT CYBER CRIMES

1. Cyber Hacking

i. Meaning of Hacking

Crime in the computer generated superhighway is the new phenomenon in contemporary scenario. In our daily life we cannot think of any intellectual and necessary work without Information Technology. But this new multimedia technology is being misused and abused by deviants and criminals. Hacking attack on Bhaba Atomic Energy Centre, AIIMS, World Trade Centre etc. are examples of cyber hacking causing more harm to human life than traditional crimes. Therefore, to secure our daily life, business and every intellectual conduct we have to think of prevention and control of cyber crimes and specially of most dangerous one that is cyber hacking.

The Information Technology Act 2000 does not define “cyber crimes”. We may define cyber crimes as prohibited human conduct in computer generated superhighway or related to computer generated activities as well as related to other electronic devices which are Information Technology friendly, e.g., mobile phone, wireless, TV with internet connection etc. in the era of communication convergence. Those conducts are prohibited by State through Chapter-XI of the Information Technology Act, 2000 which is widely amended in the year 2006 and other related laws for example the Copyright Act, 1999 in India. Sections 43 and 66 of the Information Technology Act, 2000 deal with hacking and other cyber crimes and prescribe punishments. The Computer Misuse Act, 1990 in the United Kingdom and the Computer Fraud and Abuse Act, 1986 in the United States of America prescribe punishments for unauthorized access; the European Convention, 2000 recognized cyber hacking as cyber crime and so forth.
Hacking in cyberspace is not only national but also international legal challenge which requires global standard security measures and controlling policy through worldwide intensive study and research.

Hackers usually represent themselves as –

a. the protector of vulnerable and insecure information; and
b. their activities are within legal boundaries; and
c. that they are not always law-breakers.

This may be because they are confident that –

a. Very few or only a few victims are interested to lodge complaint against them.
b. Most of the times victims are unable to identify them. This is due to unspecified and undefined jurisdiction in cyber world. The accused generally commit crime thousands and thousands of miles away.
c. Again another advantage for hackers for which they repeat crime commission is that it is very much complex to understand crime in cyberspace. For example, hackers view one webpage and by deep linking get information which are very confidential without the consent of owner and download it intentionally and dishonestly; it is a complete case of theft u/s 378 of the Indian Penal Code, 1860 that if any person with dishonest intention takes away any movable property from one place to another place without the consent of owner or possessor it is theft.
d. It is also very difficult to identify and understand the unauthorized use which is criminal trespass u/s 441 of the Indian Penal Code, 1860 as well as hackers who cause damage, after data or change data etc. Therefore, expert hackers think that cyberspace is their exclusive zone and they can do anything whatever they wish very tactfully. They not only cause harm to technological and economic dominion but also to the social, cultural and political values.

In the Film ‘Hackers’ in the year 1995, Richard Gill played by Wendell Pierce, the Chief law enforcement officer says “Hackers penetrate and ravage delicate private and publicly owned computer systems, infecting them with viruses and stealing sensitive materials for their own ends. These people …. are terrorists.”

---

hyperbole with which hackers are represented and the shallowness with which hackers are understood. He had suggested that hackers are as like as rapists.

In United States v. Edward Cummings,\textsuperscript{25} it was held that mere possession of technology which is unauthorized use is a crime. In this case Ed. Cumming was identified as a “danger to the community” for being in possession of a “red box” which is a small modified Radio shack speed dialer. The device was altered to emit-ones to allow making of telephone calls free of costs from public pay phones. This was unauthorized use of telecommunication service and he was charged for the same.

\textit{R. v. Gold,}\textsuperscript{26} in the UK; Mr. Verma IIT, Kharagpur hacking of ex-employer’s source code and thereafter arrest by Central Bureau of Investigations in India with the help of Federal Bureau of Investigations in the USA; Ankit Fadia’s Denial of Service Attack case in India etc. are example that hacking causes threat to social mechanism and pause social progress which is a global legal challenge and there is an urgent need to prevent and control hacking world-wide.

\textbf{ii. Hackers—nature and character}

According to Helen Nissenbaum\textsuperscript{27} hackers never were part of the mainstream, but their current reputation as villains of cyber space is a far cry from the early days when first and foremost, they were seen. With their deviant behavior, hackers also serve to remind the technological vulnerability and ignorance in our society along with law enforcement officials and legislators. In 1960s hacking started with Telephone systems and services as phreaking and immediately spread to computers, computer system, and network.

According to Webster’s Dictionary\textsuperscript{28} ‘hacker’ means “a computer enthusiast who is especially proficient or a computer user who attempts to gain unauthorized access to computer systems.” Webster’s II New Riverside University Dictionary\textsuperscript{29} defines ‘hacker’ as “one who gains unauthorized usually non-fraudulent access (use) and those (sic) who enjoy investigating computer operating systems.” Bruce Sterling, the author of the Hacker Crackdown, observed that the term ‘hack’ ‘can signify the freewheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can be described as the determination to make use of computers and information as free and open as

\textsuperscript{25} Nos. 95-320, 8\textsuperscript{th} June 1995.
\textsuperscript{26} \textit{R. v Gold}, [1988] 2 WLR 984
\textsuperscript{27} See Supra note 21, p.40
\textsuperscript{28} Randon House (2nd Ed.) \textit{Webster’s Dictionary} (Bulletin Books, 1996)
\textsuperscript{29} 1990, Legal decision against the legion of Doom Hacker Group
possible; and can involve the heartfelt conviction that beauty can be found in computer, that
the fine aesthetic in a perfect program can liberate the mind and spirit’. 30

The new Hackers Dictionary presents following 2 basic principles hackers live by:
a. The belief that information sharing is a powerful positive good and that it is an ethical
duty of hackers to share their expertise by writing free software and facilitating
access to information and to computing resources wherever possible.
b. The belief that system cracking for fun and exploitation is ethically all right as long as
the cracker commits no theft, vandalism or breach of confidentiality. 31

iii. Hackers’ culture

Several criminologists have attempted to understand and examine the reasons of
hacking or why hackers indulge in delinquent behavior. Hackers are becoming so
uncontrollable that it has become very difficult to cope up with the situation worldwide.
Hackers originally were computer professionals who adopted the word hack as a synonym for
computer work executed with a certain level of craftsmanship. Thereafter they gradually
became desperate to spread usefulness and accessibility of computer and computer system
among general people.

But nowadays hacker and hacking have changed their meaning dramatically. To hack
means to break into or sabotage a computer system and a ‘hacker’ is the perpetrator of such
activities. Legal meaning of hacking is associated with the act of obtaining unauthorized
access to programme or data held on a computer system or alter, modify or delete etc. any
computer programme or attempt to do so.

The term Hacker is used to describe any one of the following:
a. HACKERS. They knew computers ins and out. They can make the computer do nearly
everything they want it to do.
b. CRACKERS. They break into computer systems and security thereof.
c. CYBERPUNKS. They are the masters of cryptography.
de. PHREAKERS. They combine their in depth knowledge of the Internet and the mass
Telecommunication system. 32

32 Cyberpunk and Hackers, http://www.accessoral.net/cyberwar/cyberpunk.htm
According to SRI International,\textsuperscript{33} who studied more than 80 hackers and their associates in the year 1996 in the United States of America and Europe, ‘the concept of honorable pursuit of hacking earlier had largely disappeared’.

In the year 1994 ‘Master Spy’ case\textsuperscript{34} posed a major threat to the US security system. The military chiefs feared that an East European spy ring had successfully hacked into American Air defense systems and thereby learned some of its most confidential intelligence secrets. After 13 months due inquiry and investigations it was found out that a 16 years old British music student was responsible for these break-ins. The accused, known as Data Stream ‘Cowboy’ had downloaded dozens of military files including details of their research, development and other confidential information. He had also used a company’s network of California for more than 200 logged security breaches by using a 1,200 computers and modem. He was tried and convicted in 1997 and was fined $1,915 by a London court.

iv. Possible ways of hacking

a. There are various possible ways of hacking of which one is for the malicious hacker to physically enter into the premises of others containing the computer and impersonate its owner. That is like criminal trespass u/s 441 of the Indian Penal Code. Such impersonation is very easy if the owner has no protective and security system with secret password to start or initiate operating system.

b. Even the intelligent hacker may be able to guess password where it is required by using password cracking tool. Password cracking tool tests many passwords, find it if written somewhere else, observe it during use i.e., shoulder surf.

c. If this fails and the hacker cannot start the computer without a proper or correct password then hacker can reinstall the operating system. This process of hacking is little more difficult and time consuming, but not impossible.

d. Another way to gain control is for the malicious hacker to deceive the legitimate user into entering and executing a Trojan horse programme in the computer. A Trojan horse programme contains computer instructions unknown to the user that it perform the hacker’s attack.

e. Again the hacker may take advantage of a known vulnerability of a computer operating system such as UNIX or Microsoft Windows which is most technical

\textsuperscript{33} See Supra note 28, pp. 162-163.

method and requires detail knowledge of the operating system unless a prepackaged search tool such as SATAN.  

f. Password is not only a contributory factor for hacking but also an unauthorized access tool. Password may be called as unauthorized access device; though its main function is to identify person or relate with individuals by giving them identity in cyber world. Password contains secret, personal information or personal identity. Nowadays we have to have password for everything e.g. for e-mail, ATM machines, Websites, administrators, credit cards, online banking, brokerage, web auctions, microwaves, cable boxes, garage, door, openers, bags etc. Password crackers are highly sophisticated and keep trying words, letters, and symbols combinations until hits the right one. Sometimes they have knowledge about that person and about his or her personal particulars whose password they are going to crack and use those particulars till it hits the right answer to open.

g. Use of mathematical algorithms in an attempt to break the password hash or cryptographic scheme is another way of cracking as well as to protect the password itself. Most of the hacker sites therefore, contain large numbers of password cracking programmes e.g., UNIX, Win_9X, Zip files, chat software, e-mail software.

h. Most of the times hackers target servers because vital information are stored rather than their client’s machines. A Hacker prima facie tries to operate the internet and the telephone networks. Hackers also use scanning process to scan hosts internet activities for remote vulnerabilities through quick fiber-optic connection. Malicious hackers actually focus to attack and crack the installed firewall of a net work. Therefore, whether password or PIN number or Social Security Number (SSN) every such number must be kept in head and not in writing anywhere. To prevent password cracking it is to be changed from time to time.

i. Hacking may be done by sending messages through e-mail, websites, mobile with several offers and pornographic accesses and asking their password or social security numbers and personal information.

j. Jim Falls Worth worked mutually with hackers to understand the goals of the penetration testing as others call it as friendly hacking. And he comes out with some

---

steps and procedures which criminal hackers use without owner’s permission. These are as follows:

(a). They assess the strength and weaknesses of banks new services and how they relate to the rest of the bank’s operations.
(b). They try to determine what vulnerabilities exist within those systems.
(c). They offer solutions to increase the security of the systems.
(d). They demonstrate the possibility of losses to bank or its clients by breaking into the bank.

The kinds of information upon which hackers are interested are\(^3^7\) as follows:

(a). Operating systems.
(b). Open technique and systems in use.
(c). Major vendors used within the enterprise.
(d). Physical address of data center and telephone centers.
(e). Phone exchanges information etc.
(f). Another way of attack is denial of service attack as developed in recent past.
(g). Hackers may hack for evidence when they find out that their activities are under investigation then they try to delete investigators file.

v. Hackers group

Hackers, virus writers, unauthorized users in cyberspace have no organization as traditional criminal group. Hackers generally change their password, methods, sites, group membership and e-mail address. Therefore, it is very difficult task to track hackers and hackers group. Teenagers to older people, poor to rich people, again school going children to engineers and men as well as women are involved in hacking and other cyber crimes. This is major threat and shock in the cyberspace.

Hack-Tic conferences in the Netherlands, Deacon Meetings in Las Vegas by hackers group or hacker party e.g. the Galactic Hacking Party 1989, the Hacking at the End of the Universe (HEU) Conference in 1993, the Hacking in Progress (HIP) Conference in 1997 etc.\(^3^8\) shows that hackers do have their group, they are very keen to gathering together, meetings, conferences and so forth.

vi. Changing nature of hacker’s culture


\(^{3^7}\) *Ibid.*

a. **First generation hackers**

They were computer science experts or engineers who wanted to act for public interest.\(^{39}\)

b. **Second generation hackers**

They mostly dealt with telephone services, tampering source code to cause injury computer, computer system and network.\(^{40}\)

c. **Third generation hackers**

They were mostly young people who committed hacking as fun, game, entertainment, revenge and to make money quickly.\(^{41}\)

d. **Fourth generation hackers**

It is the contemporary scenario where hackers are crackers, denial of service attackers, person who clone telephone and internet connections, cyber-terrorists and spammers. They are elderly, young, female, male, educated, uneducated etc.

From 1st to 4th generation hackers activities are different, thus they are members of heterogeneous group.

vii. **Cracking, phreaking and hacking**

When hackers cause grievous or dangerous harm to computer and computer system or network security system and break systems they are called crackers. They not only commit criminal trespass or unauthorized access but also commit other crimes. Crackers usually try to attack server where they will easily find vital information of numerous users. They therefore target through internet and telephone network. Phreakers were generally telephone hackers. They illegally enter into computer system through phone.

They illegally enter into computer systems for several purposes e.g. information and sale it out of curiosity or to make fun or game. Phreakers engage in pranks/phreakes by altering phone system, call diverting, rearranging web pages. They do so sometimes without any aim to gain financially though their activities cause loss to corporate bodies, Industries, Government Departments, Individuals and so forth.

---

40 *Id.* at pp. 158-184.
Phreakers are forefathers of hacks and hackers. Prior to computer our communications mostly depended on telephone. In public telephone where facilities are available to call by inserting one Rupee coin, people do commit such crime. They carefully slid the strip down the slot as far as it may go and pick up the phone and while get a dial tone they put a coin into the slot and as the phone registered the coin and call was made, immediately they do get back their coin. Thus they make free telephone calls through a piece of stiff construction board which is cut accordingly and is adjusted with slot.
viii. **Hackers’ behaviour**

Most of the intensive study of criminologists in the contemporary hi-tech society is based on hackers and hacking. Several criminologists have attempted to understand hackers’ behaviour and to examine the causes for which hackers are involved in delinquent behaviours and to develop effective legal principles for the prevention and control of this dangerous crime.

Some jurists say that hackers commit crime due to passion or tendency or addiction to use computer and to act with network e.g., hacker Bedworth in 1993 was arrested in England and his advocate took defence that he was suffering from a psychological addiction and irresistible impulse to use computers, computer systems and network on which ground he was acquitted.\(^4\)

According to Winn Schwartau hacking is an intense experience. Someone cannot say one day, “Hey, hacking is cool. I want to be a hacker and then go to do it. After devotion of several months and years for learning computer systems, network, programming and software one may become hacker. Because, at one point, the skilled hacker will prevail, and the network will be his. The truly skilled, creative, and original hacker will spend his every available waking moment ... and access to computers ... no matter his true motives. He will learn from his mistakes, be cautious in his endeavors, and perfect his techniques. Perhaps he will build better hacking tools to speed up his tasks, automate the redundant steps, and build alternatives for attacking different kinds of computers. And all of this takes a lot of time.”\(^5\)

Hackers are most of the times male teenagers, who are and were neglected children at their early age, habitually, addicted for drugs and alcohol they are generally very smart but with poor educational performance, they are pleasant and representable personalities with patience to sit well at the keyboard and monitor hours after hours.

ix. **Ethical hacking**

Certified ethical hackers are hired when companies want someone from outside to test their systems for penetration by illegal hackers. Software engineers, B.Sc. (Computer Science) graduates, anyone with understanding of programmes and codes and knows how to

---


exploit a system are into ethical hacking. They ensure online security to IT companies, patrol internet highways plugging holes and preventing online crime.\(^{44}\)

x. **International Initiatives to Prevent and Control Cyber Hacking**

a. **The European Union**

The European Committee (EC) on Cyber Crime Problems formulated a committee of experts on crimes in cyberspace and they made a draft Convention on Cyber Crimes, Draft No.25 REV.5, on December 2000, which was followed by the Cyber Crimes Treaty on 23rd November 2001. This was the first International Treaty with about 45 signatories to specifically target the cyber crimes.

The Convention provides for Substantive Criminal Law.\(^{45}\) It consists of offences such as hacking, virus attack, denial of service attack etc. It prohibits illegal or unauthorized access,\(^{46}\) illegal interception,\(^{47}\) data interference,\(^{48}\) system interference,\(^{49}\) and misuse of devices.\(^{50}\)

The Convention provides for procedural law for investigations, prosecutions, searches, seizors and other conditions with safeguards\(^{51}\) and it also deals with jurisdiction issues.\(^{52}\)

The Convention deals with International co-operation with general principles and principles relating to extradition, mutual assistance etc. for the prevention and control of cyber crimes. These uniform guidelines are very much helpful to reduce cyber hacking.

It provides for settlement of disputes that the European Committee on Crime Problem (CDPC) shall be kept informed regarding the interpretation and application of this convention. And that in case of a dispute between parties to the interpretation or application of this convention, parties shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC as an

\(^{44}\) "These Hyderabad Techies Hack from the Right Side", *Indian Express*, September 4, 2008, p. 5
\(^{45}\) Convention on Cyber Crimes; Section 1
\(^{46}\) Ibid., Article 2
\(^{47}\) Ibid., Article 3
\(^{48}\) Ibid., Article 4
\(^{49}\) Ibid., Article 5
\(^{50}\) Ibid., Article 6
\(^{51}\) Ibid., Section 2
\(^{52}\) Ibid., Section 3
arbitral tribunal whose decisions shall be binding upon the parties, or to the International Court of Justice, as agreed upon by the concerned parties.\textsuperscript{53}

It provides for the consultations of the parties periodically for the effective use and implementation of this convention, exchange of information, prevention and control of hacking and other cyber crimes.\textsuperscript{54} It also provides that the parties shall inform the Committee about the result of consultations.\textsuperscript{55}

b. The Global Internet Liberty Campaign (GILC)

It brings draft proposals to empower the law enforcers to intercept international communications and traffic data with the hope to give police forces free range to wire tap or to access internet users to prevent and control abuse. Though, Walter Schwimmer (Secretary of EC) objects that this proposal allows the free hand for investigations without first establishing controlling measures if they have done something wrong. This measure is open to abuse by law enforcement bodies. One proposal of the treaty was to outlaw “hacking tools” with internet security tools. Again GILC members say that this would impose unnecessary restriction on the legitimate promotion of computer security technologies.

The challenges that law enforcement agencies face in our battle with cyber crimes are generally being divided into following 3 categories:

- **Technical** – that hinders law enforcement ability to find and prosecute criminals operating online.
- **Legal** – resulting from laws and legal tools needed to investigate cyber crime lagging behind technological, structural and social changes.
- **Operational** – to ensure that we have created a network of well trained, well-equipped investigators and prosecutors who work together with unprecedented speed even across the national borders.\textsuperscript{56}

The global nature of the internet is the contributory factor for hiding identity and cyber crime internationally. For example, a computer hacker in the UK might attack the computers of a corporation located only a few miles away or in India, France and the USA. The situation is very complex for the law enforcing agencies to investigate and arrest criminals who wave

\textsuperscript{53} Ibid., Article 45
\textsuperscript{54} Ibid., Article 46
\textsuperscript{55} 18\textsuperscript{th} January 2005 published with title ‘A man in Court on International Computer Crime Charges” in http://www.cyemos.org/newsline/.html
communication through multiple countries. What is most important is the international co-operation and assistance; without this, deviants will commit crimes freely again and again.

xi. **Cyber hacking in the United Kingdom**

While explaining situation of hacking in the United Kingdom (UK), Professor L. Lloyd says,\textsuperscript{57} “the stereotypical depiction of a cyber hacker tends to be that of a male teenager in a greasy T-shirt and torn jeans who spend hours slumped over a terminal, eyes gazing fixedly at the green glow of the VDU monitor.... No where is safe, no one can keep him out, no one knows of the scale of the threat, the silent deadly menace stalks the networks as seen in *R v. Gold.*”\textsuperscript{58}

a. **Audit Commission**

On the basis of prevention is better than cure, the UK Audit Commission recommended some preventive measures with the British standard for information security management. The reports identified certain security polices which are very urgent to follow:

a. Cyber security which is adequate with business strategy.

b. Clear statement of the importance of cyber security.

c. Clear statement of the adequate and proper law regarding Information Technology security.

d. Clear statement of the responsibilities of staff to protect investment in new Technology and computer data.

e. Clear statement of the steps taken by the management to encourage to adopt and maintain high security standards as well as to enforce it in reality by the management.

f. Statement of the steps taken to reduce computer misuse i.e. secure password systems etc.

g. Statement of data processing through new hardware and software.

h. Internal control mechanisms.

These all are with the tune of the British Standard for Information Security Management (BS 7799) such as key controls, security document, education and training, responsibilities, reporting, virus controls, data protection etc.\textsuperscript{59}


\textsuperscript{58} (1988) AC 1060.

\textsuperscript{59} The Audit Commission Reports, *Ghost in the Machine: An Analysis of IT Fraud and Abuse*, 1998 Publications, p. 3; See also David Bainbridge, *Introduction to Computer Law*, 4\textsuperscript{th} Ed., 2000, pp. 351-352. For detail see [http://www.ZDNetNews.com](http://www.ZDNetNews.com), 4\textsuperscript{th} April, 2001/5.00 PM/PT.
b. **Cyber hacking before 1990**

In the United Kingdom before the Computer Misuse Act, 1990, there were laws like the Theft Act, the Telecommunications Act, 1984 prohibiting misuse of the public telecommunications. The Interception of Communication Act, 1985, prohibits forgery and other criminal activities in the course of transmission by the public telecommunication systems. The Data Protection Act, 1984 was passed to protect computer data and database from any violations or damage.

In *R. v. Gold*, 60 two computer hackers gained access into the British Telecom Prestel Gold computer network without permission and altered the data. One of the accused also accessed the files of the Duke of Edinburgh’s personal computer and left there a message “GOOD AFTERNOON HRH DUKE OF EDINBURGH”. Both the hackers were journalists. Their claim was that they had hacked into the network in order to highlight the deficiencies in its security system. They were charged u/s 1 of the Forgery and Counterfeiting Act, 1981, because they made the false instrument with intention to use it to induce others to accept it as genuine one. To fulfill this end they had committed hacking. They hacked Customer Identification Numbers (CIN) and password. Under section 8(1) of the said Act though the instrument is recorded or stored on disc, tape, soundtrack or other device but it can be treated as false instruments. Therefore, the crown court held the accused guilty and imposed $750 and $600 fine respectively. Appeal court quashed their conviction and this was confirmed by the House of Lords. The appellate court with the Lord Chief Justice Lane said that “the accused’s act of dishonest trick to gain unauthorized access to the British Telecom files were not criminal offence. However, they may be convicted for deceiving a computer; and deceiving a machine is not possible and not an offence under the Theft Act.” The House of Lords confirmed this sensible judgment and declared hacking as not only an illegal act but also a crime which needs to be curbed immediately.

Therefore, the House of Lord’s appointed the Law Commission for their recommendations and suggestions to make law to prevent and control hacking in the year 1988. They submitted their report in the year 1989 with recommendation to enact specific law on Computer Misuse in the UK.

c. **Cyber hacking in the year 1990**

---

60 [1988] 2 WLR 984
The Computer Misuse Act, 1990 introduces following 3 new criminal offences:

- **Unauthorized access to computer material.** This is similar to using a computer without permission i.e. hacking with intention or knowledge which has connection with other computer.

- **Unauthorized access to computer material with intent to commit or facilitate commission of further crimes.** This is to be called as more malicious hacking or cracking.

- **Unauthorized modification of computer material.** These are prohibited u/s 3 of the said Act. The Act prohibits conspiracy to commit the above mentioned offences u/s 6.

d. **Cyber hacking after 1990**

   In *R. v. Crop*, Aglion, J. held that the Computer Misuse Act, 1990 will be applicable only when one computer is used to access another computer.

   In *DPP v. Bignell*, the issue raised was that, even where a person is authorized to access computer data if he exceeds his authorization and thereby access computer data for unauthorized purposes, whether he will be guilty of the unauthorized access u/s 1 of the Act 1990. In the instant case, two police officers used the computer and took information from a police database and used this information for their private purposes. The Divisional Court of the Queen’s Bench Division held that their conduct did not constitute unauthorized access because they were very much authorized to control access to the material in question.

   In *R v. Whitaker*, court referred to section 3 of the Computer Misuse Act, 1990 i.e. unauthorized modification of computer materials by the hackers. Here the defendant developed a software which he transferred to complainant. The defendant then, believed that he had retained the software copyright. Therefore, he also believed that he was entitled to insert a logic bomb into the software in order to prevent its use. But in fact there was no contract between the parties to the dispute about the retention of copyright by the defendant ‘Whitaker’. The court held the defendant guilty of unauthorized modification of computer material u/s 3 of the Act of 1990.

---


63 The Times, 6th June 1997, QBD

In Strickland and Woods case, Honorable Harris, J. explained that there may be people who consider hacking as harmless but it is not so. Computers now-a-days play a central role in our life i.e. of personal details, financial details, confidential matters of companies and Government departments, business organizations etc. It is essential to protect those integral detail information from hackers because hackers put those integrity into jeopardy.

The Confederation of British Industry (CBI) on a survey reported that with the increasing scenario of cyber hacking, the development of e-business in Britain is also facing problem. The CBI also reported that two-third of the companies had experienced cyber attacks such as hacking, virus, credit card fraud etc. Therefore, they proposed to the British Government to act cordially and to help to tackle cyber crimes, to create a centre for cyber crimes complaints, and to expand and extend the Computer Misuse Act, 1990 to cover attacks that cause the failure of Information Technology system.

xii. Cyber hacking in the United States of America

a. Legislative approach

The United States of America (USA) enacted several Federal and State Laws for the security system and to control and prevent cyber crimes for example, hacking, tampering source documents, cyber theft, cyber fraud, cyber terrorism, cyber pornography etc. by and through computer, computer system and computer network.

The Spyware Control and Privacy Protection Act, 2000 is such an Act to prevent and control hacking in the USA. The Act prohibits any deceptive activities relating to Spyware i.e. unauthorized use of the protected computer and causing other crimes thereby are prohibited. In such case the authorized user cannot open the internet browser unless closing all the programmes or turning off the computer or diverting the internet browser. Therefore, this is a kind of Denial of Service (DOS) attack. The Act also prohibits unauthorized modification of computer settings, network, and web page. Punishment prescribed under the said Act is a fine of $3,000,000 and a penalty of $1,000,000.

---

67 For details see http://www.thomas.loc.gov/cgi-bin/query/Fc 108.4.
68 The Spyware Control and Privacy Protection Act, 2000; Section 2(1)
69 Ibid., Section 2 (2)
70 Ibid., Section 4
The Computer Fraud and Abuse Act, 1986 deals with unauthorized access to computer, computer system and computer network in the United States.

b. **Judicial approach**

In *United States v. Morris*, the law involved was Section 2(d) of the Computer Fraud and Abuse Act, 1986; Title 18 USC Section 1030 (a) 5 (A) which prescribe punishment for intentional unauthorized access of “federal interest computers” and causing damage or prevents authorized use of information in such computer, causing loss of $1,000 more. In this case, the accused, released into the internet, a national computer network, a computer programme known as ‘Worm’ which differs from ‘Virus’ and it caused ‘Crash’ and ‘Ceased functioning’ of computers at various educational institutions and military websites. The Northern District Court convicted him under Title 18 USC Section 1030 (a) 5 (A). Morris then preferred an appeal before the Circuit Court. The Circuit Court concluded that Section 1030 (a) 5 (A) does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss. There was sufficient evidence for the jury to conclude that Morris acted ‘without authorization’ within the meaning of Section 1030 (a) 5 (A). Morris was sentenced to 3 years of probation, community service for 400 hours and a fine of $10,050.

In *United States v. Torricelli*, the U.S. attorney announced that Raymond Torricelli of 21 years old, “a/k/a rolex” a member of a hacker group known as “# conflict” was pleaded guilty in Federal Court to charges of the breaking into two NASA Jet Propulsion Laboratory computer located in California. The accused used one computer to host an internet chat room and to access password, username and installed programmes. In the year 1998 he admitted that he was a member of said hacker group who used “rootkit” i.e. a programme which allows a hacker to unauthorized access. One of the computer he accessed with intention to commit hacking was used by the National Aeronautics and Space Administration (NASA) and another was used by the Jet Propulsion Laboratory’s (JPL) Communications Group systems section. The accused after breaking also invited chat room participants to view pornographic images and earned about $0.18 for each visit. He was also pleaded guilty of intercepting user names and passwords of computer network of San Jose State University to gain free internet.

---


access and to steal more computers. Even when encryption was in action he used to use “John-the-ripper” programme to decrypt the passwords. He was also guilty of credit card numbers theft. Therefore, District Court imposed sentence of 4 months imprisonment, 4 months home confinement and to pay a $ 4,400 in restitution to NASA.

In *United States v. Amato*, Amato was charged for violating the regulations and orders of the administration of NASA. He was the contract employee of NASA, Ohio and without authority downloaded ‘Zipped computer file’ called ‘ZIP-42’ from internet and transmitted it to an e-mail account on the NASA e-mail server 7 times to cause international damage of about $ 12,000. Statutory punishment for violation of Title 18 USC Section 799 and NASA’S Rules and Regulations is up to 7 years in prison and $ 100,000 fine or both.

In *United States v. A. Lamo*, Lamo was pleaded guilty by FBI before the Manhattan Federal Court that he has been committing hacking into the internal computer network of the New York Times. The accused also accessed a database containing personal information including telephone numbers and Social Security Numbers of more than 3,000 contributors of New York Times OP-Ed Page. The Times immediately filed complaint against Lamo. He was charged under Title 18 USC sections 1030 and 1023. Punishment prescribed for Lamo was 5 years imprisonment and $250,000 fine by the District Court.

In *United States v. Mr. Meydbray*, the accused was formerly the Information Technology Manager of Creative Explosions, Inc. He was indicted by Jury for gaining unauthorized access to his former employer’s computer system, reading e-mail, damaging computer network etc. The maximum statutory penalty prescribed for unauthorized communication and damage is 5 years imprisonment and for causing intentional damage to a computer is 10 years imprisonment and fine of $250,000 or twice the gross gain or loss whichever is greater for each offences.

In *United States v. Mr. Lyttle*, Lyttle pleaded guilty in Federal Court in Oakland for hacking Government computers and thereafter defacing Government websites. He also obtained data illegally and caused damage above $70,000. He was charged under title 18

---

73 (N.D. Ohio) 13th February 2003, 1A/US Department of Justice, press release
74 (S.D.N.Y.) 8th January 2004, CI 3000 K private, US Department of Justice, press release; For detail see [http://www.justice.gov/criminal/cybercrime/Lamo/rolex.htm](http://www.justice.gov/criminal/cybercrime/Lamo/rolex.htm)
USC Section 1030 and was sentenced to 4 months in federal prison, $72,000 damages and to serve 3 years supervised release after prison period.

xiii. **Cyber hacking in India**

In the globalised, liberalized era of communication convergence and new technology, the server is in one State and user in other State. The application of law in cyberspace is very complex due to undefined Jurisdiction. It is international as well as national legal challenge. India enacted the Information Technology Act, 2000 following the United Nation’s Model Law, 1997. The Information Technology Act, 2000 specifically Section 43 and 66 deal with hacking and unauthorized access to computer, computer system and computer network.

The term ‘hacking’ is synonymous with unauthorized access and criminal trespass. Hacking is associated with the act of obtaining unauthorized access to programme or data held on a computer, computer system, computer network or alternative, modification, deletion, destroy of any computer programme or attempt to do such unauthorized access. Therefore, hacking is a prohibited conduct which is prohibited by State through criminal law i.e. the Information Technology Act and the Indian Penal Code in India, and State prescribes punishment for hacking through criminal law.

According to a recent study entitled ‘Shadow in the Clouds’ conducted by the University of Toronto, Canada it is revealed that China has been able to hack India’s secret diplomatic documents and defence information. However, China has rejected this report and said that we are opposed to hacking and consider it as an international crime. 77

a. **Essential elements of hacking**

Following are the essential elements of hacking:

(a). Causing intentional wrong or damage to other.
(b). Causing wrong or damage to other with knowledge.
(c). It must relate to computer, computer system or computer network.
(d). The result must be to (a) destroy (b) delete (c) alter (d) diminish the value or utility of information or (e) affect injuriously.

So, what is most important here is “Intention” or “Knowledge” i.e., ‘mens rea’ or guilty mind and ‘actus reus’ or human conduct as in the maxim ‘actus non facit reus nisi mens sit rea’. It means actus reus unaccompanied by mens rea is not a crime. The maxim is

very much applicable for hacking in cyberspace. On the other hand “presumption of innocence until proved guilty” must not be applicable here. Burden of proof is not on prosecution rather it must be on alleged accused who have to prove their innocence that they had no intention or knowledge to commit hacking and that they had taken all possible and reasonable precaution to prevent and control hacking. It is very difficult to prove intention and knowledge in digital environment and intention is question of fact and not of law. Therefore, it may be judged from every circumstance.

b. Legislative Approach in India

- **Civil Liability**

  The information Technology Act, 2000, deals with penalty for damage to computer, computer system and computer network without the authority from owner, in-charge or other authorized person and even abetment for the same.\(^{78}\) The term “damage” is defined as destroy, alter, delete, add, modify, rearrange any computer resource by any means.\(^{79}\) The unauthorized access to resources, downloading and flowing viruses, damage, disruption, denial of services, tampering or manipulating and abetment of these are punishable with maximum Rs. 1 crore as liability to pay to victim as compensation.\(^{80}\) The civil remedy which is available to victim is to be adjudicated by the Cyber Appellate Tribunal. All the proceedings are to be according to the Indian Penal Code 1860\(^ {81}\) and tribunal shall be deemed to be a Civil Court.\(^ {82}\)

- **Criminal Liability**

  In contemporary progressive and dynamic social phenomenon, every law is in development so we hope it is also true for the Information Technology Law. Several areas of the Act of 2000 are not very clear, for example, what is wrongful loss is not defined though it is defined in the Indian Penal Code, 1860.\(^ {83}\) It does not define the terms such as destroy, alteration, delete, hacking. Unauthorized access is relevant in criminal trespass which is defined in the Indian Penal Code, 1860 as: “Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property or, having lawfully entered into or upon such property,

---

\(^{78}\) The Information Technology Act, 2000; Section 43

\(^{79}\) Ibid., Explanation (iv)

\(^{80}\) Ibid.

\(^{81}\) Indian Penal Code 1860; Section 193 and 228

\(^{82}\) Supra note 75, Section 46 (5) and 58 (2)

\(^{83}\) Supra note 78, Section 23
unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit ‘criminal trespass’.

In *Smt. Mathri v. State of Punjab*, the court held that to establish criminal trespass mere entry in others property is not enough rather he must have knowledge of subsequent annoyance and must have entered intentionally to commit further crime. But when hackers enter into others computer, computer system even without intention to commit further crime, only unauthorized access information which may be exploited by him or not; he will be punished u/s 66 of the Information Technology Act, 2000. And the Act provides for search and seizure of the computer and other storage devices out of the possession of the hacker. This is because, our data or information is so valuable and delicate that only access may diminish its importance.

The Information Technology Act, 2000 define ‘hacking’ as: “Hacking with computers system (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to 3 years or with fine which may extend up to Rs 2 lakh or with both.”

The Act also prescribes punishment for sending offensive messages through communication service, etc. “Any person who sends, by means of a computer resource or a communication device, (a) any content that is grossly offensive or has menacing character; or (b) any content which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes use of such computer resource or a communication device, shall be punishable with imprisonment for a term which may extend to 2 years and with fine.

The receiving and retaining stolen computer resources and information which includes computer, mobile, communication device, digital signals of TV Transmission and the like, is prohibited. Thus, “whoever dishonestly receives or retain any stolen computer resource or communication device knowing or having reason to believe that the same to be a stolen computer resource or communication device, shall be punished with imprisonment of

---

84 The Indian Penal Code, 1860; Section 441
85 AIR 1964 SC 986; (1964) 5 SCR 916; (1964) 2 Cr LJ 57
86 The Information Technology Act, 2000; Section 66
87 Ibid., Section 66 A
either description for a term which may extend to 3 years or with fine which may extend to Rs. 1 lakh or with both.\textsuperscript{88}

The identity theft is prohibited as “whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term that extends up to 3 years and shall also be liable to fine which may extend to Rs. 1 lakh.”\textsuperscript{89}

Cyber cheating is also prohibited as “whoever by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1 lakh.”\textsuperscript{90}

\begin{itemize}
  \item **Jurisdictional Riddles**
  
  The Act is applicable to prevent and control cyber hacking (a) even outside India, (b) committed by any person irrespective of his nationality. This Act shall apply to an offence committed outside India by any person if it involves a computer, computer system or computer network located in India.\textsuperscript{91} Accordingly, only reasonable link with computer, computer network, computer system located in India is enough to define cyber jurisdiction to combat cyber hacking. The word ‘reasonable’ makes jurisdictional problem more complicated. Reasonable in one case may not be so in other circumstances. If it is according to prudent thinking, judiciary is the proper forum to determine which are reasonable and which are not. In India we can hardly visualize judicial decision on Cyber Hacking.

  \item **Procedure**
  
  The Controller is empowered to give direction to Certifying Authority or any employee of such authority to take necessary steps to prevent and control cyber hacking and other cyber crimes. And when any one fails to comply with this Act, Rules or Regulations, he shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding 3 years or with a fine not exceeding Rs. 2 lakh or with both.\textsuperscript{92}

  \item **Powers of the Police and other Authority**
\end{itemize}

\textsuperscript{88} \textit{Ibid.}, Section 66 B
\textsuperscript{89} \textit{Ibid.}, Section 66 C
\textsuperscript{90} \textit{Ibid.}, Section 66 D
\textsuperscript{91} \textit{Ibid.}, Section 75 (2)
\textsuperscript{92} \textit{Ibid.}, Section 68 (1)
Confiscation of computer system and related devices for violation of this Act is allowed.\textsuperscript{93} A police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.\textsuperscript{94} The Police Officer and other Officers are empowered to enter, into any public place and search and arrest without warrant any person found reasonable suspected or guilty of commission of the crime or of committing or attempted to commit any offence under this Act.\textsuperscript{95}

c. \textbf{Socio-legal impact of cyber hacking in India}

    Cyber hacking does not mean no loss to human life because hackers are human being and they are causing injury to human society. Especially Bhabha Atomic Research Centre servers and traffic control servers were hacked, which are direct examples of injury to human life. On 11th September 2001 and July 2005 recent attack on the USA and the UK are burning, painful and measurable instances in contemporary scenario which has impact of cyber hacking and cyber terrorism.

    Former CBI Director Mr. R.K. Ragavan\textsuperscript{96} said that it is very difficult to nail on Pakistani hackers because the Indian hackers are not conniving with the Pakistani law enforcers. Therefore any prudent person can think about the kind of cooperation India may get from Pakistan. Hackers generally break-in and steal information from computer system by using software, who have thorough knowledge of that software. In the year 2000 about 635 Indian websites were hacked. It was very complex phenomenon to even identify hackers. People of India are most the times illiterate and reluctant about this crime and complaint. Mr. Dewang Mehta, President of NASSCOM says that the lack of uniform laws against cyber crimes involving abuse of computer systems made prosecution of cross-border hackers difficult.\textsuperscript{97}

    \textbullet\textbf{ Delhi Hacker’s Case:} Delhi Police arrested two hackers on 6\textsuperscript{th} February 2001.\textsuperscript{98} It was the most breaking news in India because two people were arrested by the Delhi Police for allegation of hacking a website. This was probably the first case in India where accused were arrested. Both the hackers were detained for allegedly blocking the website

\textsuperscript{93} Ibid., Section 76
\textsuperscript{94} Ibid., Section 78
\textsuperscript{95} Ibid., Section 80
\textsuperscript{97} National Association of Software and Service companies; For details see http://www.BBCNews.com/10thJanuary2001/News
\textsuperscript{98} Ibid.
named www.goZnextjob.com. This website provides support and information to prospective employers and job-seekers. The accused posted a message on that website declaring that it was closed but actually it was very much open. The hackers were sent to judicial custody for 14 days as they were charged u/s 406 of IPC, 1860 i.e. criminal breach of trust, and u/s 66 of the IT Act, 2000 i.e. offence of hacking.

➢ **Hacker Dr. Neruker:** On 5th July 2001 the Cyber Crimes Investigation Cell Mumbai received an unknown telephone that their website www.ccicmumbai.com is going to be attacked by hackers. Immediately Police Officers noticed that it has been hacked. They identified the hackers who replaced the original homepage of the Mumbai Police website and posted there obscene comments and abuses to Police Officials. The Police Officers then investigated their server room i.e. Net4India and had taken help of the members of Advisory and Technical Committees to analyze the log records. They investigated that Internet Protocol address which was related to this hacking belonged to the internet provider company DISHNET SSL LTD, Mumbai and the end user of that same date and time was identified by internet provider immediately. It was a cyber cafe i.e. “Osprey Enterprises” at Dadar, Shivaji Park. Police entered into that cyber cafe and proceeded their search and examination of computers, at last they found out the copy of their homepage in a computer which was replaced and related to software cute FTP. Then Mumbai Police seized that computer and took the descriptions of the culprits who used the computers. Immediately the police drew the sketch of the suspected accused. After investigation the police arrested Anand Ashok Khare and Mahesh Mhatre for committing hacking. Both accepted their guilt and are now working with Mumbai Police Cyber Crime Investigation Cell for the prevention and control of hacking under assumed identities as ‘Dr. Neruker’ and ‘Dr. Libran’ respectively.

➢ **Arrest of Ex-scientist from ISRO:** Even on 21st September 2001, one Ex-Scientist was arrested from ISRO for E-mail threats to the Department of Atomic Energy and hacking of an Internet Service Provider, Icenet at Ahmedabad, India and also for sending e-mail threat to the nations security which is also to be treated as cyber terrorism.

---


**Arrest of Computer Trainers at Chattisgarh:** One Manoj Singania, head of the local branch of Aptech and another Prakash Yadav, in-charge of training institute were arrested for allegedly sending e-mails in the name of Microsoft and Videsh Sancher Nigam Ltd. (VSNL) India. Those e-mails were containing programme file named ‘Speed.exe.’ At the moment file was opened it would automatically sent to accused the password, data and other information of the user. They had also tried to hack into the computers of the State Bank of India (SBI) in the same way.

**Mr. Bhardwaj Case:** In 2001, Mr. Bharadwaj, Managing Director of IGSP Technology Centre India Pvt. Ltd. filed an FIR at Chandigarh about hacking of ‘computer system u/s 66 (1) and 66 (2) of the IT Act, 2000 and u/s 380 of the IPC, 1860 that Techno Noble Info Way Ltd. (TNIL) had illegally downloaded some data from their server in the U.S. The Police officers started immediate search of TNIL office premises and confiscated the server, related devices used in the crime. Though, accused’s plea on the other hand was that IGSP committed breach of contract by not providing them minimum service as was agreed.

**IIT Kharagpur Case:** Only for co-operation and active collaboration of the Federal Bureau of Investigation (FBI), the Central Bureau of Investigation (CBI) in India arrested 27 years old software Engineer, Mr. Shekhar Verma for allegedly trying to illegally sell the ‘Source Code’ of a sophisticated software package worth about $70 million. The package was called as “Solid Works 2001 Plus”. The culprit IIT graduate, Kharagpur was caught red-handed while he was about to sale the same package to two undercover FBI agents at Ashoka Hotel. He believed that undercover FBI agents were the representatives of one US Company. Therefore, he had struck a $ 2, 00,000 deals with them for the misappropriated source code. He was a former employee of a software company called Geometric Software Solutions Company Ltd. in Mumbai. While he was in service, he took the entire Source Code and after resignation started approaching other software companies in the USA through e-mail which was treated as a very shameful act. This is also to be treated as cyber fraud committed by hacker.

---

➢ **Hacker Kalpesh Sharma’s Case:** On 26th September 2003, media news disclosed about hacker Kalpesh Sharma as he was put behind the bars in Ahmedabad. He was arrested on 24th September by the Cyber Crime Branch of Mumbai Police on a complaint filed by UTI Bank official that the accused hacked the site of UTI Banks i.e. [www.uti.com](http://www.uti.com) on 11th July and send an e-mail to the bank authority with a message that “the website is weak and they should provide security”. He expressed that he can do good for security in exchange of Rs. 15 Lakh and posted his contact numbers. Police arrested him from Ahmedabad and he was charged u/s 66 and 43 (b) of the IT, Act 2000 and remanded to Police custody.104

➢ **Banks as Prime Victims of Hacking:** One employee of Bank of India tapped organization’s computer network on 12th November 2003. The alleged accused after tapping the computer network gathered data on all keys, passwords, monitoring system and other information. He was arrested by police, though was released on bail thereafter.105

The latest in a rash of cyber break-ins that have targeted high profile companies and institutions is the major cyber attack on the International Monetary Fund (IMF) in June, 2011 aimed to steal sensitive insider information. This attack was clearly designed to infiltrate the IMF with the intention of gaining sensitive insider privileged information. The US Federal Bureau of Information (FBI) is helping to investigate the attack and it is found that the IMF had detected suspicious file transfers and also that a desktop computer had been compromised and used to access some IMF systems.106

➢ **ATM Hacking:** The complaint was filed by one private firm that the money had been withdrawn on 30th July by using a password which was hacked by accused. On 10th August, 2004, the New Delhi Police arrested 27 years old hacker Mr. Rajesh Malhotra. He was charged for hacking on ATM machine in Mayur Vihar and for withdrawing Rs. 3 lakhs. Police also seized from the accused the same amount. But he was released on bail thereafter.107

---


106 “Cyber Attack to Steal Insider Info”, *The Hindu*, June 14, 2011, p. 16

107 For details see *Times of India*, 10th August and 12th November 2004.
Online Traders Hacking: A Ghaziabad based online trader’s password was stolen by a hacker which was related to shares and caused loss of about Rs.5 lakh. Hackers were getting account information of those traders and using the same they bought shares at very high prices, but they were then selling it at very low prices which were causing huge financial losses.\(^{108}\)

Hackers Phishing: Worldwide hackers are pursuing the method of ‘Phishing’ to drive spam, Junk mail, advertisements and several offers. Bangalore Police detected only between July and December 2004 about 10,310 phishing attacks by hackers. Hackers most of the times preferred to use financial service sites, healthcare sites, online etc. to make netizens vulnerable. Symantec blocking was over 33 million a week between July to December 2004. Hackers are using spam in contemporary scenario to steal confidential information such as identities, passwords and accounts.\(^{109}\)

Baroda (Gujarat) Hacking Case: On 9\(^{th}\) June 2005, hackers attacked on one website and claimed $10,000 for restoration of website. Indian Police even became 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 which any one is going to buy from any company or institutions.\(^{110}\)

Hacking between India and Pakistan: Hacking took new shape between India and Pakistan i.e. net-war by way of defacement and control of websites of each other. In the year 2005, almost 114 Pakistani sites have been hacked by Indian hackers and about 766 Indian sites were hacked by Pakistani hackers.\(^{111}\)

Mobile Phone Hacking: In 2006 most of the hackers had started to misuse mobile phone, hacking the software and cyber spying through contemporary communication convergence technology and mobile commerce.

Hacking of official website of BPRD by Pakistan: Recently in February 2011 the Tis Hazari Court of Delhi has issued request letter to the Justice Department of Pakistan to

---


\(^{109}\) R. Raghavendra, TNN reported in the **Times of India**, 14\(^{th}\) May, 2005.


help the CBI in the investigation of hacking of official website of the Bureau of Police Research and Development (BPRD) and uploading of objectionable material thereon by Pakistan based hacker group named ‘Varzil’ in 2010. It was alleged that the website was hacked by using 4 Internet Protocol IDs and after investigation it was found that these IP addresses belong to Pakistan.\textsuperscript{112}

In August 2007, hackers developed Trojan horse, a type of virus and programmed it to send out personalized e-mails to Monster.com users known as job opportunity site and the programme asked user to submit bank details. Through this programme about 1.6 million entries such as names, detail identity, addresses, telephone numbers and so forth were stolen by hackers. Hackers used the identical way of phishing where users are very often asked to enter personal details.\textsuperscript{113}

The West Bengal National University of Judicial Sciences, Kolkata was forced to remove its website www.nujs.edu on 5\textsuperscript{th} February, 2008 as hackers linked it to a pornographic site which caused embarrassment to all visited dignitaries.\textsuperscript{114}

\textbf{xiv. Combating Cyber Hacking}

Hackers usually try to use social engineering. They also try to learn about the target technology, free tools from the internet and try to build their own tools to gather information. Therefore, we have to have more teeth and nail for preventing and controlling this which is very dynamic and complex scenario. We have to keep in mind another way to hide e-message is encryption for which always decryption must be available which brings hidden message back to normal text or plain text and then it becomes very difficult to cancel. Therefore, encryption and decryption keys must be used for sending messages and receiving messages both to communicate each other.

Teenage hackers like Ankit Fadia at 14 years, Neeraj Pattath at 17 years are appointed by the NASSCOM, Mumbai Police and other committees in India to advise (1) to set up anti-hacking measures; (2) to know how to detect hacking; (3) to know how to solve hacking problem. They are to be called as ethical hackers as Kevin Mitnik in USA. A major hack was

\textsuperscript{112}“Website Hacking Mein Pak Ke Nyaya Vibhag Ko Anurodh Patra Jari”, \textit{Dainik Bhaskar}, February 16, 2011, p. 15.

\textsuperscript{113}\textit{The Economic Times}, Kolkata, 24\textsuperscript{th} August 2007, p. 13.

\textsuperscript{114}\textit{The Times of India}, Kolkata, 6\textsuperscript{th} February 2008, p. 4.
avoided by Mr. Ankit Fadia when he was only 16 years old e.g. denial of service attacks by Pakistani hackers group etc. He detected that its origin is in Pakistan.\footnote{115}

Every computer user ought to use screen saver and system lock activities. Every prospective user of new multimedia technology ought to get essential training about prevention and control of hacking and how to maintain security system.

Though Government and law enforcing organizations are keeping their eyes to combat hacking but this is again true that hacking is increasing day by day India. It is because of some loopholes in Information Technology law and great illiteracy about the subject amongst the people. Definitely, lack of awareness is vital contributory factor for hacking. Our judiciary also needs some training and infrastructure developments in this field. To achieve the objectives of the cyber law, Indian judiciary may use ethical hackers to find out drawbacks of technology, to help investigation of cyber crimes and thereby to assist prevention and control of cyber crimes.

Hackers culture, modes of hacking are almost synonymous worldwide whether in Russia, USA, UK, Canada, Australia, India or anywhere in the globe. Therefore, we need to adopt uniform law on jurisdiction issue. There is great need of uniform law and international co-operation to prevent and control cyber hacking worldwide. There is need to adopt uniform law worldwide because this is not only a national problem but also an international problem.

Only a police officer not below the rank of Assistant Commissioner of Police can register or investigate hacking and other cyber crimes. It means they are not easily accessible by attacked victims. And as a result most of the cases go unreported. Therefore, the rank of police must be made even below the rank of Inspector of Police. Punishment must increase at the extreme point to show deterrent effect.

2. \textbf{Cyber Fraud}

i. \textbf{Historical Background of Cyber Fraud}

The most complex challenges faced by the Government and law enforcement agencies since 1960s in the cyberspace are cyber fraud and other cyber crimes. This may be because the business world, financial sectors etc. were the most popular users of computer and internet from the early times of new multimedia technology. The cyberspace becomes a

media for the fraudsters where victims generally cannot recognize the accused. Therefore, cyber frauds become the most pervasive form of white collar crime worldwide.

On 5th March, 2000 about 19 people were charged for chat room fraud which caused about $ 8.4 million loss in New York. In India instance of Pune based Business Processes Organizations (BPO) fraud in April 2005, Karan Bahrees cyber fraud case in June 2005 etc., are instances that cyber fraud is increasing day by day and there is immediate need to prevent and control this complex problem worldwide.

ii. Meaning of Cyber fraud

The term “cyber fraud” is not defined in the IT 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.\(^{116}\)

The Audit Commission of the United Kingdom (UK) defined ‘cyber fraud’ as “any fraudulent behaviour connected with computerization by which some one intends to gain financial advantage”.\(^{117}\) The United States Department of Justice describes “telemarketing fraud” as the use of telephones, internet, cell-phone etc. to deprive victims dishonestly of money or property or to misrepresent the value of goods or services”.\(^{118}\)

Therefore, we can say, “any dishonest, fraudulent activities in cyberspace using new multimedia technology in the era of communication convergence for wrongful gain and to cause wrongful loss to the victim which is prohibited by the Criminal Law and for which State imposes punishment is cyber fraud”.

iii. Possible modes of cyber fraud

a. Cyber fraud due to victim’s excitement

Victim’s excitement is one easy way to commit cyber fraud. Most of the times, victims are attracted and motivated to facilitate the schemes in cyberspace e.g. cyber

\(^{117}\) The Audit Commission of the UK since 1987-90 study report, Para 7
marketing, e-banking, e-shopping and the like. These schemes are most of the time much misleading and victims are excited to these.

b. **Personal identities and password fraud in the cyberspace**

In cyberspace the offenders pretend that they are victim’s good friends and they try to convince victims with intention to access their personal information so that these can be used by the accused to commit cyber fraud i.e. credit card withdrawal, fraudulent money transaction, bank account fraud, ATM fraud etc.

c. **Cyber fraud by false representation**

The offenders in cyber space also represent falsely that they have authority to do something for or on behalf of the victims or they are the Government officials. By this way they access the personal identity and commit cyber fraud.

d. **Cyber fraud using urgency**

“Urgent” is the term the fraudsters often use with some advertisement or statement which shows scope to win prize if invested by the potential victims.

e. **Cyber lottery fraud**

Cyber lottery scheme is one way to commit cyber fraud which require investment in tickets to give chance to win prize. It may also be called as cyber gambling.

f. **Credit scheme fraud in cyberspace**

Credit scheme to offer loan in exchange of fees, interests, taxes, service charge etc. is one way to commit cyber fraud.

g. **Travel related scheme**

Cyber shopping, telefunding, telemarketing etc. are also ways to commit fraud in cyber world.

h. **Electronic-mail fraud and Internet fraud**

In January 2005, a mass e-mail was posted to help Tsunami disaster victims but it was in fact a way to spread computer virus, to initiate a Denial of Service attack against a German website. The worm appeared was “Tsunami donation! Please help!” which also invites recipients to open an attachment called “Tsunami.esec”. If anyone opens it then it will forward the virus to other internet user. Innocent users were into a belief that they are helping for Tsunami disaster.\(^{119}\)

iv. **International initiatives to combat cyber fraud**

Cyber fraud is not only national legal challenge but also international legal challenge. Therefore, the European Council (EC), the United Nations (UN), the United States of America (USA), the United Kingdom (UK), India, Bangladesh, Pakistan and other countries are adopting intensive study and research project with the object to evolve uniform and effective legal system to prevent and control cyber fraud worldwide.

a. **The European Union**

The European Committee on Crime Problems and Committee of Experts on Crime in Cyberspace drafted Convention on Cyber Crimes which was published on 22nd December 2000 with the aim to adopt and enact uniform criminal policy to protect society against cyber crimes. It prohibits computer-related forgery\(^{120}\) and computer-related fraud\(^{121}\). It provides that each party to the European Council must adopt appropriate legislative and other measures to establish cyber fraud as criminal offence under their domestic law if committed intentionally and without rights causing loss to others property.\(^{122}\) It also defines cyber fraud as “any input, alternation, deletion or suppression of computer data; any interference with the functioning of a computer or computer system with intent to procure unauthorized economic benefit for self or others and causing loss to others property is cyber fraud”.\(^{123}\)

b. **United Nations**

The United Nations Commission on International Trade Law adopted 51/162 MODEL LAW on Electronic Commerce which is applicable to any kind of information in the form of a data message used in the context of commercial activities. Following the said law several countries enacted and modified their national laws e.g. the USA, the UK, India, Israel, Russia, Australia, Canada, Bangladesh, Pakistan etc.

v. **Cyber fraud in the United Kingdom**

David Bainbridge has said that “as far as the criminal is concerned, the creation of an account in his own name, followed by instructions via a computer terminal to the main computer to transfer large sums into that account, is much more attractive than walking into a

---

\(^{120}\) The Convention on Cyber Crimes; Article 7  
\(^{121}\) *Ibid.*, Article 8  
\(^{122}\) *Ibid.*  
\(^{123}\) *Ibid.*
bank with a shotgun” \textsuperscript{124}. He categorized computer fraud mainly into 2 types (a) data fraud and (b) programme fraud. Data fraud includes unauthorized data entered into a computer or alteration, or suppression of data.

The UK Audit Commission identified 4 types of cyber fraud, namely (1) input fraud, (2) output fraud, (3) programme fraud, (4) data fraud.

\textbf{a. Input fraud}

It is related to the false data or falsification of data at the time of or prior to its entry into a computer. This is extremely extensive form of computer fraud. In the case of conspiracy \textsuperscript{125} between Local Government wages clerk and about 20 employees, clerks made false electronic entries on the computer time sheets which resulted additional payments to the workers. It was shared by the clerks. The scheme was continued for 3 years. That was a complete case of cyber fraud through input. Input fraud is one way of unauthorized alteration of data before it is being put into a computer. This can be prevented and controlled by regular review, auditing and checking the systems as well as modifying and enhancing the auditing system by the organizations and authorities.

\textbf{b. Data fraud}

This is a kind of alteration of input data. In data fraud the person who is entering the data into the computer makes changes to the data. It can be controlled by appropriate checking procedures and auditing system by the authorities. \textsuperscript{126} The National Audit Office reported a case in 1995, where a member staff in an employment department entered false data relating to a claim by the brother of the accused. His brother received the amount of value 2933 pound of which he was not at all entitled but it was possible due to his false entry. The accused employee was dismissed and prosecuted. The accused employee was, thereafter, convicted and was sentenced to 2 months imprisonment for committing computer fraud.

\textbf{c. Output fraud}

This type of fraud is related to output computer data, be it printed or not printed but suppressed or altered or modified. May be input to computer was not deceptive but deception has been caused to the output of computer data.

\textsuperscript{124} David Bainbridge, Introduction to Computer Law, Ed. 2000, Ch. 24, P. 291.
\textsuperscript{125} Case 2 cited in the Audit Commissions Survey 1984-87 as Survey case.
\textsuperscript{126} The National Audit Office reported a case in 1995; IT Security in Government Departments, HM SO, 1995, at 17.
In *Adams v. Queen*,\(^{127}\) two company Directors concealed information relating to secret profits they had made from the company they worked for, by the use of offshore companies and Bank accounts. One of the Directors brought an appeal to the judicial committee of the Privy Council against his conviction in New Zealand on the charge of conspiracy to defraud, and the appeal was dismissed.

d. **Programme fraud**

It is more grievous because here, to commit fraud, the perpetrators change the computer programme itself. In *R. v. Thompson*,\(^{128}\) the accused, a computer programmer, was employed by a Bank in Kuwait. He made plans to defraud the Bank. He knew that deal accounts were maintained on computer electronically. He devised a programme which instructed the computer to transfer sums from these accounts to his newly opened Bank account. He then returned from Kuwait to England to minimize the risks of detection and then opened a number of accounts with English Banks and wrote request letter to the Bank Manager in Kuwait to arrange to transfer his balance from Kuwaiti accounts to English Banks accounts. But subsequently he was detained by police on charge of computer fraud by deception and was convicted.

---

\(^{127}\) 4\(^{th}\) November, 1994 (cur-reported) cited in, D. Bainbridge, *Introduction to Computer Law*, 4\(^{th}\) Ed. at p. 293.

\(^{128}\) [1984]1 WLR 962
e. **Internet fraud**

The National Criminal Investigative Service published a report in 1999 on internet fraud. Project Trawler suggested in this report that “in the majority of cases, traditional methods of fraud e.g., misuse of credit cards, failure to deliver goods ordered and paid for, pyramid selling, pump and dump share pushing have been given a new lease of life on the internet.”¹²⁹

The Institute of Chartered Accounts for England and Wales, Fraud Advisory Panel in 1999 reported that losses in the UK out of internet fraud might range from about 400 to 500 pound. However in the United States in February 2000, the internet fraud watches report mentioned¹³⁰ in website that consumers lost over $ 3.2 million to internet fraud in 1999 as reported to the National Consumers Leagues Internet Fraud Watch.

Nevertheless, computerized payment and Electronic Funds Transfer (EFT) systems become very popular now-a-days especially in the business world due to globalization and liberalization. The Scotland Yard’s Computer Crime Unit’s ex-head has commented as follows “the prevention of crime here is important. No, it’s not important, it’s vital, these days money is not the pound in your pocket, it’s the $ 234 billion worth of transactions which go out from the city of London and back every day. All that money really amounts to is electronic digits travelling down wires. That’s real money.”¹³¹

In *R v. Gold*,¹³² one system called “the Prestel System” was the main dispute. It gave facilities to its subscribers to access database services, e-mail and others in rental payment basis and further charges if required. It used to recognize its users through their passwords and identification numbers. This password and identity information was available only to a British Telecom engineer for his work. This was tapped by accused Gold and he used the password so extensively that the British Telecom suspected misuse. They recorded telephone numbers of Gold and other information which was retained on the Prestel computer. The accused was tried at South Work Crown Court, and convicted with fine. He lodged appeal against his conviction. The Court of Appeal¹³³ concluded that “the appellant’s conduct amounted in essence… to dishonestly obtaining access to the relevant Prestel data Bank by a

---

¹²⁹ For details see [http://www.ncis.co.uk/contact.html](http://www.ncis.co.uk/contact.html).


¹³¹ Guardian, 9th January.

¹³² [1988] 1 AC 1063 (HL) & at [1987] 3 WLR 803 (Court of Appeal)

¹³³ [1987] 3 WLR 803 at 809
trick. This is not a criminal offence. If it is thought desirable to do so, that is a matter for the legislature rather than the Courts, we express no view on the matter”.

In Re, Bignall case, a police officer had used for the purpose of investigating the data containing identity of a motor vehicle owner from the police national computer. It was proved that this personal information had nothing to do with police investigation. Therefore, the police officer was charged u/s 1 of the Computer Misuse Act, 1990, though the use of computer was authorized. The contention of the respondent counsel was that the primary purpose of the Computer Misuse Act, 1990 was to protect the integrity of computer systems rather than the information. And that a person who causes a computer to access and was entitled to gain access does not commit an offence even if he performs a function to secure access to information held at a level to which he intends to secure access for an unauthorized purpose. It is only where the level of unauthorized access has been knowingly and intentionally exceeded that an offence will be committed, provided the alleged person was known about that unauthorized level of access. The Divisional Court accepting the submission of the counsel for the respondent held that the respondent had committed no offence under the Computer Misuse Act 1990.

vi. Cyber fraud in the USA

The USA enacted the Computer Fraud and Abuse Act, 1986 which was amended twice in the year 1994 and 1996 and again changed by the Patriot Act, 2001 after terrorist attack on World Trade Centre and Pentagon on 11th September 2001.

The Federal statute Title 18 US Code Section 1030 deals with the fraud and related activities in connections with computers. It has following 3 goals:

(i) confidentiality,
(ii) Integrity
(iii) Availability of the data or communications.

To achieve above goals the 1986 Act prohibits using computer to commit following seven crimes:

(i) Accessing information without authorization or exceeding authorized access knowingly to commit espionage.
(ii) To access information without or exceeding authorization.
(iii) Unauthorized access to non-public Government computer.

---

134 [1998] 1 Cr App Rep 1
(iv) To access any computer to commit international fraud.
(v) Knowingly or intentionally damage a computer.
(vi) Traffic in password with knowledge.
(vii) Threatening to cause damage to a computer with intention to extort money or other valuable things.\(^\text{135}\)

*United States v. Morris,\(^\text{136}\)* is one of the landmark cases in the USA which deals with cyber fraud. Morris, the accused was held guilty of violating Title 18 U.S.C. section 1030 (a) (5) (a) by the Jury in trial. Morris was authorized to use computers at Cornell, Harvard and Berkeley. He was authorized to communicate through internet to other computers, computer system and network. He was authorized to send e-mail, collect information etc. He transmitted “worm” which was considered as exceeding authorized access or unauthorized access. It was proved that he used send-mail and connect other computer and by this way unauthorisedly accessed other computer. In fact he found holes in programmes which gave scope to him for a special and unauthorized access route into others computer. He was sentenced to 3 years of probation, 400 hours of community service and fined with $ 10,050. He appealed to the Circuit Court against the decision of the trial court. Section 1030 (a) (5) (a) of the Computer Fraud and Abuse Act, 1986 provides that whoever knowingly causes the transmission of a programme, information, code or command and as a result of such conduct, intentionally causes damage without authorization to a protected computer be punished. Morris contended that his conduct was almost exceeding authorized access but not unauthorized access. And the evidence was also not sufficient to convict him of unauthorized access. The Circuit Court affirmed the District Courts Judgment.

In *United States v. Czubinski,\(^\text{137}\)* the accused Czubinski was one of the employees of the Taxpayer Services Division (TSD) at Boston. He regularly accessed information from TSD as part of his duties. He used his valid password and search codes to get income tax information of several taxpayers in the United States. This was prohibited by special rules and under Title 18 U.S. Code sections 1029 and 1030 i.e., exceeding authorized access and

\(^{135}\) For detail see [http://www.businesscredit.com](http://www.businesscredit.com); Unlimited documents and cyber fraud by Cara Washington 2004, 20\(^{th}\) April. See also [www.consumerfraudreporting.org/stolenchecks.htm-183k](http://www.consumerfraudreporting.org/stolenchecks.htm-183k). See also [ieeexlore.ieee.org/ie15/4509594/4509595/04509853.pdf?isNumber=4509595&prod=CNF&arNumber=4509853](http://ieeexlore.ieee.org/ie15/4509594/4509595/04509853.pdf?isNumber=4509595&prod=CNF&arNumber=4509853).

\(^{136}\) 928 r.2d 505 (2d cir), Cir Court denied, 502 U.S. 817 (1991). For detail see [http://www.usdoj.gov/atr/cases/indx144.htm](http://www.usdoj.gov/atr/cases/indx144.htm).

\(^{137}\) 106 F3d 1069 (1\(^{st}\) Cir. 1997); For details see [http://www.usdoj.gov/criminal/cybercrime/ ccmanual/01ccma.html](http://www.usdoj.gov/criminal/cybercrime/ ccmanual/01ccma.html).
unauthorized access to commit cyber fraud. He was not permitted to access file on its systems exceeding his official duties. He carried out several unauthorized searches of files knowingly but he was not authorized for the same. However, there was no evidence about the discloser or sale of those information. But, in a jury trial he was convicted for computer fraud. He appealed against this conviction before Circuit Court. The Circuit judge opined that unquestionably the accused exceeded authorized access, to a federal interest computer, though the accused argue that he did not obtain “anything of value”. But the value of information depends on needs and objectives and whether it is valuable to the accused in the light of fraud is to be proved which Government failed. Therefore, it may be caused out of curiosity. The Court held that no rational Jury could conclude beyond reasonable doubt that the alleged accused intended to use or the same as obtaining something of value for the purpose of the Computer Fraud and Abuse Act, 1986. And Czubinski has not obtained valuable information to fulfill the fraudulent scheme. Therefore, the court reversed the defendant’s conviction on all counts.

vii. Cyber fraud in India

In contemporary era of communication convergence, online money transaction, e-banking, e-shopping, internet auction, internet lottery, data conversation, data transfer to online ticket booking and in almost all aspects of our life, we have to walk on the superhighway. So, we have to go through cyberspace.

a. Legislative Approach

➢ The Indian Penal Code, 1860

Several provisions of the IPC, 1860 are relevant which prohibit and prescribe punishment for fraudulent activities. The IPC has been amended to give effect to the IT Act, 2000, specially provisions relating to cheating and dishonestly inducing delivery of property or valuable security,\(^\text{138}\) forgery,\(^\text{139}\) punishment for forgery,\(^\text{140}\) forgery of valuable security,\(^\text{141}\) using as genuine a forged document\(^\text{142}\) etc. The word ‘fraudulently’ has been defined in the IPC as “a person is said to do a thing fraudulently if he does that think with intent to defraud,

\(^{138}\) The Indian Penal Code, 1860; Section 420

\(^{139}\) Ibid., Section 460

\(^{140}\) Ibid., Section 465

\(^{141}\) Ibid., Section 467

\(^{142}\) Ibid., Section 471
but not otherwise.”

Therefore, these provisions of the IPC are helpful to prevent and control cyber fraud.

➤ The Information Technology Act, 2000

Several provisions of the IT Act, 2000 are relevant for the prevention and control of cyber fraud in India though they do not define cyber fraud.

When any person without authorization from the owner or any competent person who can give permission accesses, downloads, copies or extracts any data, computer data base or information from any computer, computer network, computer system, computer data or data base or data stored in removable medium i.e. CD, Floppy, DVD and so forth or causes similar damage, he shall be liable to pay maximum Rs. 1 crore compensation.

• Elements of crime in cyber fraud

The punishment is prescribed for intentionally and knowingly tampering with computer source code or source documents, computer system, network etc. without the permission of the owner or authorized person. Herein 2 elements of crime are present (i) mens rea or guilt mind and (ii) actus reus or act. The mens rea in cyber fraud are knowingly or intentionally and actus reus which relate to human conduct such as conceals, destroys or alters etc.

• Tempering source code

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years, or with fine which may extend up to Rs. 2 lakh, or with both.

• Jurisdictional riddles

The application of the IT Act, 2000 to prevent and control cyber fraud, cyber hacking and other cyber crimes committed within or outside India, committed by any person irrespective of his nationality is dealt within the Act itself. This Act shall apply to an

---

143 Ibid., Section 25
144 The Information Technology Act; Section 43 (b)
145 Ibid., Section 65
146 Ibid., Section 65
147 Ibid., Section 75 (1)
offence committed outside India by any person if it involves a computer, computer system or computer network located in India. Therefore, jurisdiction is one of the complex problems in the cyberspace to control cyber fraud and other cyber crimes though the CPC, the Cr PC and the IT Act, 2000 provide that place of business or residence or registration of corporation or computer server will be treated as location for cause of action.

- **Powers of the police**
  
  i. Confiscation of computer system and related devices for violation of the IT Act, 2000 is allowed under the Act.
  
  ii. A police officer not below the rank of Deputy Superintendent of Police shall investigate any offence.
  
  iii. Police Officer and other Officers are empowered to enter into any public place and search and arrest without warrant any person found reasonably suspected or guilty of commission of the crime or of committing or attempted to commit any offence under the IT Act.

- **Liability of Network Service Providers (NSP)**

  The Network Service Providers are not liable for any other persons information or data made available by him if NSPs can prove innocence and that they had taken all reasonable or due diligence to prevent such crimes.

---

148 Ibid., Section 75 (2)
149 Ibid., Section 13
150 Ibid., Section 76
151 Ibid., Section 78
152 Ibid., Section 80
153 Ibid., Section 79
• **Fraud relating to Electronic Signature Certificate**

The misrepresentation or suppression of any material fact from the Controller or Certifying Authority for obtaining any license or Electronic Signature Certificate is punishable with imprisonment which may extend up to 2 years or with fine of Rs.1 lakh or with both.\(^{154}\)

When any person knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purposes, he shall be punished with imprisonment which may extend up to 2 years or with fine which may extend up to Rs.1 lakh or with both.\(^{155}\)

b. **Socio-legal impact of cyber fraud in India**

> **Hyderabad’s Rs. 20 Crore Data Conversation Fraud**

Mr. C. Suresh, the Managing Director of Vinsri Infotech and owner of the website *InfoTech Pvt. Ltd.* had started his business in 1997 of data conversion, to give data entry works, to provide services for data entry, medical transcription, management and e-Books etc. In January 2002, he fraudulently received Rs. 2.5 lakh non-refundable deposits from each of the clients giving false promise to give data entry work.\(^{156}\) And in February 2003, when cheques issued to his clients by him were not cleared rather dishonored because funds were not available; his clients started demanding either refund of their deposited amount or clearance of their bills and to provide work. But Mr. C. Suresh, the accused was silent. Therefore, his clients went to police and lodged separate complaints. Then he was arrested from Secundrabad on the charge of cyber fraud i.e. about Rs. 20 crore data conversion fraud.

> **Bangalore Cyber Fraud Case**

The Sutra Solutions with 42 branch offices were working as Call Centre and had taken more than 400 students and others promising them to give jobs after few months. They were taken as trainees. The Sutra collected from trainees Rs. 6,000 as customer support and Rs. 25,000 for technical support; total Rs. 1.2 crore from all. After depositing the said money some of the trainees identified that the Sutra’s website named [www.sutrasolutions.com](http://www.sutrasolutions.com) was going down, they were not paying building rent and telephone rents were due. Thereafter the victims lodged complaints against the company. Ajay Shah (CEO) had been absconding and

\(^{154}\) *Ibid.*, Section 71  
\(^{155}\) *Ibid.*, Section 74  
police arrested Mr. Raju Krishnamurthy on the charge of cyber fraud though thereafter he was released on bail.\footnote{For detail see http://www.ciol.com.news, 8\textsuperscript{th} May 2003, Advertisement. See also http://www.rediff.com/money/2003/may/10cybercafe.htm.}

\begin{itemize}
\item \textbf{Click Fraud}

This is a kind of cyber fraud related to clicking on web search advertisements by users who have no aim to do business with advertisers. In web the company who puts the advertisement has to pay for each click by users to the web-search providers, for e.g. Google, Yahoo and Rediffmail etc. These web-search providers, therefore, use machines and people to make more clicks on advertisement and for which they will earn money from the advertisers.\footnote{For detail see http://www.cnetnews.com, 30\textsuperscript{th} June, 2005 by Renters. See also http://en.wikipedia.org/wiki/click_fraud.}

\item \textbf{Pune Cyber Fraud Case}

About 16 accused were arrested in the incident of Pune cyber fraud. Young employees of BPO industry Mphasis – Msource were the accused. They defrauded the United States based Citibank customers of more than Rs. 1.5 crore, including damage to data. John Varghese, a 31 years young was the master mind of the story. The accused were authorized to access the confidential information of Citibank account holders as the bank was the e-banking service providers. The accused accessed password/PINs information from about 5 account holders. Thereafter the culprits have started their operation by sending and diverting e-mails of e-banking funds transactions. The victims were only receiving about funds transfer nothing else. One of the victims then lodged complaint to the Citibank and then Citibank alerted the Mumbai and New York City Investigative Services about the same. Mumbai Citigroup immediately reached recipient banks in Pune and alerted the Pune Police’s Cyber Crime Cell to trap the cyber fraud. The accused were caught red-handed while they were about to check the fund transfer in a Rupees Co-operative Bank, Pune. The accused were charged u/s 65, 66, 71 and 72 of the IT Act, 2000 and u/s 420, 465, 467 and 671 of the IPC, 1860.

\item \textbf{Karan Bahree’s Case}

The sting operation of the British Tabloid through their newspaper ‘The Sun’ seemed Indian BPO industries very cloudy in the end of June 2005. On 24\textsuperscript{th} June 2005, a Journalist of
'The Sun' newspaper expressed that he had obtained account numbers, secret passwords, credit card details etc. of almost 1000 British Bank customers from Karan Bahree, the employee of a BPO firm at Gurgaon by paying 3 pounds. This 24 years old Mr. Karan Bahree was employed only before 3 months of the incident on probation as a Junior content writer with infinity e-search. He did not have authority to access those confidential information said by his employer. Subsequently, Karan was fired from the job. Karan delivered a Compact Disk (CD) to Mr. Oliver who was from the UK as the undercover reporter of British Tabloid Newspaper. But, no complaint has been registered to control and punish this culprit with the economic offence wing of the Delhi Police. Karan Bahree’s case was dealt with u/s 43 (b), 65, 66, 72 and 74 of the IT Act, 2000.

After Karan Bahree’s case in June-July 2005, Prime Minister Dr. Manmohan Singh directed NASSCOM to amend and adopt more effective Data Protection Laws, security measures and to increase penalties for cyber crimes in superhighway with the tune of the UK, the USA and to adopt International standard of security system to prevent these instances in future. Dr. Singh said that “Indian professionals have built for themselves an enviable global reputation through hard work, dedication and commitment, and the occasional misguided acts of some individuals should not be allowed to damage the high reputation of all professionals.

➢ Lottery Fraud and Cyber Squatter

Most of the times we receive electronic mails information that we are going to win or we won a prize in a lottery. To receive lottery money the recipients of letters or e-mails naturally sent their reply. As they will send reply again they will receive another e-mail asking information about bank accounts, mode of transactions they prefer and other confidential information. They do charge money as processing fee before that fund transfer. But that prize in lottery to recipient’s accounts never happened and on the other hand his confidential information, bank accounts etc. may be misused or abused for commission of other crimes.

➢ West Bengal Cyber Fraud Case


160 June 29, New Delhi, India, Published in Times of India, Kolkata, 30th June, 2005. See also http://www.NDTV.com News 29th June 2005.
The Kolkata Police raided about 792 online lottery units and 7 district units on 19th December 2004. The State Finance Department sought police force on 17th December to control violation of the Lotteries Regulation Act, 1998. The Police seized about 472 electronic lottery devices in Kolkata and investigated that most of them do not have trade licences.

**HSBC, Bangalore Cyber Fraud Case**

The accused who was a resident of Bangalore joined HSBC on 12th December 2005 producing forged certificates. He had links with terrorist groups and the underworld groups. He was arrested on charges of data theft and cyber fraud. He committed data theft to illegally transfer money from account of a multinational and the UK based Bank’s customers. HSBC Electronic Data Processing India Pvt. Ltd., Bangalore was the Bank’s BPO arm. They had lodged a complaint with the Cyber Crime Police Station (CCPS) against that cyber fraud. The crime was so dangerous in nature that the HSBC’s technical team from Hyderabad as well as Interpol section of police department became involved to investigate and control it.

**Kolkata Cyber Fraud Case**

Sulagna Roy, a 23 years old NIFT educated call centre employee committed cyber fraud through calcuttaweb.com. Her nature of work was selling dish TV to US client. During her work she collected credit card information of those clients and then started purchasing more than 52 items worth Rs. 1.8 lakh (\$4,000) by using laptop internet and cyber cafes internet, these items were including jewellery, sarees, chocolate, air-conditioner etc. The calcuttaweb.com provided details of purchases to Detective Department and CID at Kolkata. She only earned Rs. 8,000 monthly but was buying that valuable thing. She was arrested and charged with fraud and cheating. She confessed that she did it for fun but not to commit any intentional crime.

**Cyber Fraud traced by Detective Department of Mumbai**

The owner of Mumbai based e-portal NS Shop-mart named ‘Sidhartha’ was arrested in the month of September 2006. Sidhartha committed cyber fraud and e-commerce cheating with Supriyo Roy of Barasat at West Bengal. Through http://www.rediff.com Supriyo Roy had purchased an LCD monitor and paid Rs. 15,000 in favour of Sidhartha. But, the LCD was never delivered to Supriyo, rather a cartoon stuffed
with paper reached his home a few days later. The police found Sidhartha’s portal from rediff.com and brought him back to Kolkata after arresting him from Dadar, Mumbai.  

➢ **Nigerian Scam in Delhi**

Recently, the Special Operation Squad of the Delhi Police Crime Branch cracked Nigerian gang in Delhi which was involved in cyber fraud. They used to send fake mails through internet, which appeared to be genuine mails sent by banks to their customers, and used to ask their customer ID, e-banking ID, account number, and password etc. thereafter, they used to transfer the money in these customer’s account to their own account.

➢ **Abdul Kadir’s Case**

The Special Task Force of U.P arrested 2 persons allegedly involved in internet fraud and cheating people of hefty amount. They used to trap their clients by sending them e-mail luring them in the name of their selection for a lottery prize of $ 2 b. They also demanded money from the parties in the name of courier and VAT charges and doing insurance prior to transferring their prize amount.

viii. **Combating Cyber Fraud**

Communication convergence and new multimedia technology have become very popular in contemporary globalised and liberalized society. In 1960s the US Defense Department started using computer network, thereafter computer network was used by academic and research institutions and eventually the USA invented ICANN and Protocol system. Gradually cyber world became cloudy and complex due to its misuse and abuse by criminals. Business world is the most popular user of computer, computer network, computer software and other information process devices of modern times. Detection and investigation of cyber crimes is emerging as problem due to unspecified and undefined jurisdiction in cyberspace.

In India industries and individuals must adopt world standard security systems with anti-viruses measures to protect themselves from financial loss as well as loss of reputation in the era of liberalization, globalization and communication convergence.

---

162 “Internet Ke Istaimal Se Kiye Kale Karname”, Navbharat Times, June 30, 2008, p. 16
163 “Two held for Internet Fraud, The Hindu, December 31, 2007, p. 10
164 Internet Corporation of Assigned Names and Numbers
With Government polices and law, people of India have vital role to play if we wish to prevent and control cyber fraud. For e.g. at the time of e-business, e-shopping or e-banking while personal information along with credit card number are required or asked, we must apply our mind. Sometimes, we give all our information even money as processing fees but in reality we never receive any home delivery or otherwise from those fraudsters rather often they use our credit cards and other identities to fulfill their end.

Most of the times credit card fraud is committed when someone gives passwords or personal information numbers (PINs) to others. That can be checked by Governmental and non-Governmental Organizations, Law Universities and Colleges, Local Bodies etc. by organizing Seminars, Workshops, Cyber Legal Aid and Free Legal Awareness programmes.

Industries, companies and other business enterprises need to give their employees intensive training to make them aware about consequences of cyber crimes and ways for prevention of cyber fraud. Industries, companies and other business enterprises need to administer e-mails of their employees.

General awareness programmes need to be conducted by Government sector and educational institutions e.g. about virus scanning, maintaining identity record of every net users by ISPs, deletion of important data after use, keeping password in brain, granting membership to net users by ISPs and cyber cafes, running anti-virus software, using filter system and firewall software, effect of abuse and misuse of multimedia technology and the like.

3. **Cyber Pornography**

i. **Meaning of Cyber Pornography**

Morality has sociological and psychological aspects. Morality is individual’s perception due to which human beings accept certain things as good and reject certain things as bad in society. It is dynamic with dynamic society. It varies from person to person and society to society. What is immoral for one is not so to other or in other society. There is no yardstick to determine what things are moral and what are immoral.\(^{166}\)

Therefore, it is left to the judiciary as reasonable and prudent repository of moral standard in society. Law and morality are closely related. When there is synthesis between

them in society, there will be no conflict and society will progress smoothly and fast. But all morals are not enforceable by law rather we have to make a balance and accept shared morality.

We have freedom of speech and expression under the Constitution\textsuperscript{167} but reasonable restriction is imposed on it to maintain decency and morality.\textsuperscript{168} Again restrictions imposed by the IPC, 1860 provide for offences against morality, decency, privacy, law and order.\textsuperscript{169} Therefore, obscenity is prohibited. In the era of information technology it is prohibited by the IT Act, 2000.\textsuperscript{170}

In \textit{Life Insurance Corporation of India v. Prof. M.D. Shah},\textsuperscript{171} the court held that this freedom is basic and fundamental right of individuals which they acquire by virtue of birth as human beings, and in a democratic country any attempt to gag this right except under Art.19 (2) is violation of democracy and Art.19 (1) (a).

The first World Congress was held in August 1996 at Stockholm. The prime issue of the Congress was Commercial Sexual Exploitation of Children. The Congress discussed about visual or audio material which exploit children sexually. Due to easy access to worldwide web through new multimedia technology, cyber pornography and other cyber crimes are increasing every moment. These pose a complex challenge for the legislation and law enforcing agencies worldwide. It became very easy to use, distribute or sell pornographic materials. These acts affect moral and psychological growth of society.

The United States of America (USA), the United Kingdom (UK), Canada, Russia, Australia, India and other countries worldwide are raising their voice to fight against cyber pornography which corrupt mind of young people and others who are sensitive to these. It demonises our socio-moral values, culture and taboos.

In contemporary social phenomenon ‘live sex’, ‘video clip’, ‘MMS clip’ etc. are also increasing day by day in Indian society be it Dr. Prakash, Delhi Bal Bharati School, Delhi Public School, Mr. Kulkarni in Pune, Nilmani Halder, Orkut controversy in Kolkata at Jadavpur, Bollywood actress Mallika, Kareena or Pretty’s case. The list is not exhaustive.

\textsuperscript{167} The Constitution of India; Article 19 (1) (a)
\textsuperscript{168} Ibid., Article 19 (2)
\textsuperscript{169} The Indian Penal Code, 1860; Section 292, 293, 499, 502, 502A, 509
\textsuperscript{170} The Information Technology Act, 2000; Section 67, 67A
\textsuperscript{171} AIR 1993 SC 171; (1992) 3 SCC 637; JT 1992 (4) SC 181
Subscribers are often asking for ‘live sex’. In case of any related ‘MMS clip’ most of the times the end users of internet view, download, transmit, save, and make printout of those images and objectionable materials as well as transmit those to others.

The Wolfenden Committee’s Report 1957\(^{172}\) of the United Kingdom recommended that prostitution as well as homosexual activities done in private between two consenting adults are not crime though immoral. Professor J.S. Mill in his book on ‘Liberty’\(^{173}\) says that unless there is harm to others in the society, State must not interfere with individual’s right or liberty. Even H.L.A Hart and Lord Devlin’s debate\(^{174}\) concluded with the shared morality, which we require for balancing democracy as well as morality in society.

ii. **International Initiatives to Combat Cyber Pornography**

The European Council’s 12\(^{th}\) Conference of Directors by the Criminological Research Institute in 1976 discussed the issue of computer-related crimes. In 1990 the United Nations Congress took special initiatives for the prevention of cyber crimes.

In 1994, a Manual on “The Prevention and Control of Computer-related Crime” was prepared and presented by the United Nations for review of Criminal Policy. The United Nations Economic and Social Council (UNESCO) took vital initiatives to combat online sexual abuse, child pornography and pedophilia and took initiatives to adopt uniform preventive and controlling measures specially on 18-19 January, 1999 at Paris with 150 participants.\(^{175}\)

In October 2000, the EU and the USA initiated a draft which is the first draft of International Treaty on Cyber Crimes. The preamble of the treaty invites for international co-operation to combat the rapid growth of cyber crimes worldwide.

In 2001, the European Council’s Committee on Crime Problems and Cyber Crimes adopted the draft convention with the initiatives of 41 nations. It contains 29 Articles. The


Convention deals with the content related offences. It prohibits child pornography and cyber pornography. On 22nd June 2001, the European Council’s Committee on Crime Problems approved the final draft of cyber crimes related convention. It provides that:

(1) Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   a. Producing child pornography for the purpose of its distribution through a computers system,
   b. Offering or making available child pornography through a computer system,
   c. Distributing or transmitting child pornography through a computer system,
   d. Procuring child pornography through a computer system for oneself or for others,
   e. Possessing child pornography in a computer system or on a computer data storage medium.

(2) ‘child pornography’ shall include pornographic materials which visually depict:
   a. A minor engaged in sexually explicit conduct;
   b. A person appearing to be a minor engaged in sexualiy explicit conduct;
   c. Realistic images representing a minor engaged in sexually explicit conduct.

iii. Cyber Pornography in the United Kingdom

Though the UK does not have any written Constitution, their freedom of speech and expressions is recognized through several laws. As we know absolute liberty will ruin society, therefore, restrictions upon the exercise and enjoyment of those rights are imposed. Those restrictions are reasonable to maintain law and order in society. However in 1727 obscenity was treated as common law offence in R v. Curl.

In Regina v. Hicklin, Lord Cockburn observed that ‘think the test of obscenity is this, whether the tendency of the matter charged as obscene is to deprave and corrupt those, whose minds are open to such immoral influences and into whose hands a publication of this sort may fall.’ This is popularly known as Hicklin test.

---

176 Title 3
177 Article 9
178 Article 9
179 [1727] 2 S 788 KB
180 Regina v. Hicklin, [1868] 3 LR QB 360; See also Uttam Singh v. The State (Delhi Administration), (1974) 4 SCC 590
a. Legislative Measures in the United Kingdom

The law on obscenity in the UK has been amended in 1994 by the Criminal Justice and Public Order Act, 1994 to control cyber pornography. The statutes i.e., the Obscene Publication Act, 1959 and 1964; the Telecommunications Act, 1984; the Protection of Children Act, 1978; the Criminal Justice Act, 1988 were changed and modified by the Act of 1994.

The Criminal Justice Act, 1988 prohibits taking any indecent photograph or pseudo-photograph of a child in his possession and prescribes punishment with an imprisonment not exceeding 6 months.\textsuperscript{181}

b. Judicial Approach to Combat Cyber Pornography in the United Kingdom

In \textit{R v. Fellows},\textsuperscript{182} one employee of the Birmingham University compiled a database of pornographic images of children without the consent or knowledge of the University. The database was stored and maintained on a computer with internet connection. This was the first case of online pornography in the UK. Herein court referred to Section 1 and 7 (4) of the Protection of Children Act, 1978; the Obscene Publications Act, 1959 and the Criminal Justice and Public Order Act, 1994. Before the Court of Appeal two issues were addressed for valuable comment. (1) Whether graphical files held on a computer fall under ‘photography’? (2) Whether a computer hard disk containing these files could be classed as an ‘article’ for the purpose of the Act of 1959? The court answered both the issues in affirmative.

In \textit{Simon Jackson’s Case},\textsuperscript{183} Simon was a computer consultant. He used to swappe photos in a ‘pernicious exchange’ with the male and female contacts abroad. He was imprisoned for 4 months by Crown court at Swindon. He was also charged for distribution of indecent photographs of children under 16 years and for possessing those with intent to distribute and for indecent assault on child. The Police force intensively investigated and carried out search procedure in his home and office computer where they found out about 2 computer towers, CD’s, modem and internet connection. Police then took help of computer expert and found out that those disks and devices contained pornographic photos of children who were preferably girls of 8 to 12 years having sex with possible young persons.

\textsuperscript{181} Section 160

\textsuperscript{182} \textit{R v. Fellows and Arnold}, [1997] 2 All ER 548; See also \textit{Atkins and Goodland v. D.P.P.}, [2000] All ER 425

\textsuperscript{183} \textit{Cases and Material related to Child Pornography on the Internet}, compiled by Yaman Akdeniz; Posted on Web page, UK sections of regulation of C.P. See also \url{http://www.cyber-rights.org/reports/ukcases.htm}.
In Father Adrian Mc Leish’s Case, the accused was a Roman Catholic Priest aged about 45 years known as Father Adrian Mc Leish. He was imprisoned by the Crown court for 6 years on the charge of collection of illicit matter in the electronic device. The Police seized 4 computers which were built by the accused. The police also found out several disks in library which almost were erased. Before arrest he destroyed most of the files and videotapes. The accused was also charged for indecent assaults against 2 boys. The accused was involved in an International paedophile on pornographic ring on the internet.

In Meechie v. Multi-Media Marketing the defendant established “the Interactive Girls Club” for the production of erotic computer entertainment with a hope that this would be appreciated among broad-minded adults. Of these one item contained a game, if any one completed that game successfully then it would display the image. That game might be isolated by expert user to go directly to obscene image display. This distribution of ‘video nasties’ is prohibited under the Video Recording Act, 1984 as it is without certificate. But the photo image was not in moving nature rather still picture. Therefore, the court held that the image will not come under ‘Video Recording’ u/s 1 of the Act of 1984. The Divisional Court reversed these findings and held the accused guilty.

In William Mckirdy’s case, the accused 31 years old driver was held guilty for online child pornography, for corrupting and depraving young girls of 9 to 14 years and for having sex with them. He was imprisoned for 12 years. Police found out 2 girls in alcoholic state, contents relating to sex aid and pornographic picture and other pornographic material stored in his computer, about 8 floppy disks which contained indecent images and CD Rom which contained pornography which was downloaded from internet.

In Robert Jone’s case, the accused was a doctor of Alternative Therapy Centre. He downloaded about 5,000 pornographic images on his computers and superimposed his own nude body on the picture. He was sentenced to jail for 4 months and his name was listed on the register as sex offender for 7 years.

---

184 Ibid.
In Mark Winter’s case, a police officer was charged with cyber pornography and was accused for making and downloading indecent child photographs from the internet.

In Wayne Barter’s case, the accused used his code name as “Bad Boy 71”. He was charged for 33 indecent images and other offences. He used to download such files to make these available to others. Police traced through his code name and searched his home. He stored such obscene and pornographic library on compact disks and computer. He was also engaged in auto-erotic sexual practices while viewing them. His name was registered as a sex offender for 10 years and he was also banned to work with children.

This is in short how the UK is fighting against cyber pornography by using their preventive and controlling measures in contemporary communication convergence era.

iv. Cyber Pornography in the USA

The First Amendment of the Constitution provides for the protection of freedom of speech and expressions in the USA. But this right is not absolute rather restricted to maintain law, social order, security and social progress. That is why defamatory statements, objectionable or obscene publications, immoral speech and expressions are not allowed.

a. Some Judgments and Incidents in the USA from 1957 to 1996

In Roth v. United States, Roth was charged as guilty for sale of books, photographs and magazines which contained obscene materials. The Supreme Court upheld his conviction and held that obscenity was not within the zone of constitutionally protected speech or press. The court also declared further that the protection to speech and press was fashioned to assure unfettered interchange of ideas to bring political and social changes designed by the people.

In 1978, the U.S. Supreme Court evolved the test for obscenity in Miller v. California. At the criminal trial it was proven that Marvin Miller is guilty of distributing obscene materials which were called as “adult materials”. He mailed these materials to the manager of a restaurant at California. That was not requested by the manager and he opened it with his mother. Then he filed a police complaint. Therefore, Miller was convicted by the

---

189 Ananova news, web page, on 29th May 2003; See also www.cyber-rights.org/reports/ukcases.htm.
jury and the State Appellate Court affirmed the same. The US Supreme Court enunciated following 3 tests:

(i). Whether the average person, applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest.
(ii). Whether the work depicts or describes, in offensive way, sexual conduct specifically defined by the State law.
(iii). Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

In United States v. Robert Thomas, the defendant and his wife operated the Amateur Action Computer Bulletin Board System (AACBBS) by using telephone, modems and personal computers. The members of it could access chat rooms, e-mails, messages, files and could transfer, download and print those files. The defendant transmitted Graphic Interchange Format files (‘GIF’) which contained pornography images. He had business relating to selling of adult video tapes to members. A police complaint was filed against Thomas. Subsequently, the U.S. Postal Inspector acts as the member of AACBBS by sending $55 and investigated the case. Thereafter defendants were tried and convicted by the federal district court for violating obscenity laws under Title 18 of the U.S. Code.

b. Legislations Prohibiting Cyber Pornography in the USA

The Communication Decency Act, 1996 was passed to protect children against pornography. Under this Act, if any person knowingly transmits obscene material for sale or distribution in the State or foreign country by using computer service, it is prohibited as criminal offence. This Act also imposes fine up to $ 100,000 and imprisonment up to 5 years for the first time offence. For subsequent offence it prescribes up to 10 years imprisonment.

The Child Pornography Prevention Act, 1996, prohibits intentional production of child pornography using new technology, transmission as well as distribution of same through online or local area network. These activities are prohibited as child pornography whether by using natural children, fictitious children or cartoons. The U.S. Code; Title 18 Section 2256

According to the U.S. Code, ‘child pornography’ is “any depiction, including any photography, film, video, picture, computer or computer generated image or picture; whether

---

194 The U.S. Code; Title 18 Section 2256
made or produced by electronic, mechanical or other means; of sexually explicit conduct; where –

(1) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(2) such visual depiction is, or appears to be of a minor engaging in sexually explicit conduct;

(3) such visual depiction has been created, adopted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct, or

(4) such visual depiction is advertised, promoted, presented, described or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.\(^{195}\)

The U.S. Code prescribes at least 15 years imprisonment for production and distribution of child pornography. And same punishment is prescribed to the recipient of the child pornography. The statute again imposes 5 years imprisonment for the possession of the same and life imprisonment for the repetition of offence by offender who was previously convicted for sexual abuse of a minor.\(^{196}\)

The Child Online Protection Act, 1998 was passed under the U.S. Code\(^{197}\) which increased the scope of the Child Pornography Prevention Act, 1996 and includes online transmissions by service providers, electronic commerce website providers as well as provides the following guidelines:

(i) Minors can access internet materials which could frustrate parental control or supervision.

(ii) Government has to take interest and initiatives to physically and psychologically protect minors from those harmful materials.

(iii) Attempts taken by industries to help parents and others to protect minors from access to those harmful materials are not successful. It ought to be successful.

(iv) The most effective and least restrictive way of protection of minors in the contemporary social scenario is prohibition of distribution of harmful material to minors combined with legitimate defence.

\(^{195}\) Ibid., Section 2256 (8)

\(^{196}\) Ibid., Section 2252 A

\(^{197}\) The U.S. Code; Title 47 Section 231
(v) Notwithstanding the existing protections prohibiting distribution of harmful materials on internet; parents, educators and industry must adopt continuous efforts to find out better way to combat the situation.

This Act prescribes punishment for commercial website operators who offer material deemed to be harmful to minors with imprisonment which may extend to 6 months and fine up to $ 50,000 or with both. The Protection of Children from the Sexual Predators Act, 1998 under the U.S. Code specifically prohibits the commercial pornographers who knowingly communicate harmful materials to the minors of 16 years or below the age for commercial purposes, or to use the internet to engage minors in sexual activities.

c. Some Judgments and Incidents in the USA after 1996

In Free Speech Coalition v. Reno, the court concluded that the definition of ‘child pornography’ under the Child Pornography Protection Act, 1996 is vague and too broad because it applied to both real as well as fictitious depictions of children. Therefore, it is inconsistent with the First Amendment of the Constitution.

In United States v. John Zuccarini, the court sentenced 30 months jail to a cyber-spammer Zuccarini for using deceptive internet names to mislead minors to X-Rated websites. The 53 years old defendant registered and used misleading domain name of several internet sites from a hotel at Florida to earn money by providing pornographic websites to the users. The domain name he misused was mainly http://www.disneyland.com as http://www.dinseyland.com. Other more than 3,000 websites which were popular with young children for entertainers, celebrities, cartoon and characters were also misused him in the similar way.

In United States v. Brain Tod, 41 years old defendant was arrested due to international investigation into child pornography on the charge of physically and sexually abusing a 6 years old girl and an infant boy to create pornographic images, thereafter posting of these on internet and hiring a man in South Carolina to kill the girl child victim and her mother.

v. Prevention and Control of Cyber Pornography in India

198 The U.S. Code; Title 18 Section 302
199 No.97-16536 (9th Cir. 17th December 1999); See also http://www.cyber-rights.org/reports/child.htm
200 The US Department of Justice, New York, Press Release, on 26th February, 2004; For detail see http://www.cybercrime.gov/zuccarinisent.htm; See also http://www.usdoj.gov/
201 News Team/AP News wire/posted in web page on 29.03.2004@05:30 via comtex. The Schedllen Berger case 2004; See also http://www.usdoj.gov / New York v. Ferber, 458 US 747
a. **Cyber Pornography and the Constitution of India**

The Constitution provides that all citizens have the right to freedom of speech and expression but in the interest of decency or morality, reasonable restrictions may be imposed on this freedom.

b. **Legislative Approach in India to Prevent and Control Cyber Pornography**

➤ **The Indian Penal Code, 1860**

The Indian Penal Code, 1860 provide for limitations and prohibitions of certain things which are obscene. It prohibits sale, distribution, publication, export, import etc. of obscene books, pamphlets, papers, writings, drawings, paintings, representations and the like except justifications like literature, art, learning, monuments, etc. and prescribes punishments on first conviction with imprisonment for a term which may extend to 2 years and with fine which may extend to Rs. 2,000 and on second conviction with imprisonment for a term which may extend to 5 years and also with fine which may extend to Rs. 5,000.

It prohibits sale of obscene objects to young persons and prescribes punishments on first conviction with imprisonment for a term which may extend to 3 years and with fine which may extend to Rs. 2,000 and on second conviction with imprisonment for a term which may extend to 7 years and also with fine which may extend to Rs. 5,000.

It further prohibits obscene acts and songs to annoyance of others in or near any public place and prescribes punishments with imprisonment for a term which may extend to 3 months or with fine or with both.

It also prohibits word, gesture or act intended to insult the modesty of a woman and prescribes punishments with imprisonment for a term which may extend to 1 year or with fine or with both.

➤ **The Information Technology Act, 2000**

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction.

---

202 The Constitution of India; Article 19 (1) (a)
203 Ibid., 19 (2)
204 The Indian Penal Code, 1860; Section 292
205 Ibid., Section 293
206 Ibid., Section 294
207 Ibid., Section 509
with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to Rs. 1 lakh and in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to Rs. 2 lakh.\textsuperscript{208}

The network service providers are not liable in certain cases if they can prove that the data provided by them was without their knowledge in spite of taking reasonable caution to prevent the offence. The burden of proof that ISPs are innocent is imposed upon service providers. For the removal of doubts, it is declared that no person providing any service as a network service provider shall be liable for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.\textsuperscript{209}

The ‘network service provider’ means an intermediary.\textsuperscript{210}

The ‘third party information’ means any information dealt with by a network service provider in his capacity as an intermediary.\textsuperscript{211}

An ‘intermediary’ with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.\textsuperscript{212}

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent under circumstances violating the privacy of that person shall be punished with imprisonment which may extend to 3 year or with fine not exceeding Rs. 2 lakh or with both.\textsuperscript{213}

\textbf{c. Judicial Response in India before the Information Technology Act, 2000}

In \textit{Ranjit D. Udeshi v. State of Maharashtra},\textsuperscript{214} the Supreme Court of India declared ‘Lady Chatterley’s Lovers’ written by D.H. Lawrence as obscene book and publication. The Court held that there is difference between ‘obscenity’ and ‘pornography’. Precise definitions are not possible. However, obscenity is any material, which tends to corrupt, cause

\begin{itemize}
  \item \textsuperscript{208} The Information Technology Act, 2000; Section 67
  \item \textsuperscript{209} \textit{Ibid.}, Section 79
  \item \textsuperscript{210} \textit{Ibid.}, Explanation (a)
  \item \textsuperscript{211} \textit{Ibid.}, Explanation (b)
  \item \textsuperscript{212} \textit{Ibid.}, Section 2(1)(w)
  \item \textsuperscript{213} \textit{Ibid.}, Section 66E
\end{itemize}
annoyance, something of horror, indecent, immoral or with sexual tendency. ‘Pornography’ means any material in writing, picture or other form, which is intended to arouse sexual desire. Both are against public morality and decency.

In Muhammed Ibrahim v. Public Prosecutor,\(^{215}\) a vendor who did not know English had in his possession 63 copies of an erotic novel called the ‘Tropic of Cancer’. The court ruled that the object of Section 292 of the IPC is to protect members of the public who may be tempted to buy these and so expose themselves to their corrupting influence. Thus, the Section must be strictly interpreted and mens rea and intention are not the essence of the offence.

In Sukanto Halder v. State of West Bengal,\(^{216}\) magazine “Nara Nari” was treated as obscene publication. To give effect to public morality about art and literature, the court u/s 292 of the IPC, 1860 convicted the petitioner and sentenced him to 2 months rigorous imprisonment and fine of Rs. 200 in default to rigorous imprisonment for 2 weeks.

In K.A. Abbas v. Union of India,\(^{217}\) the Chief Justice of Supreme Court M. Hidayatullah held regarding film censorship that our freedom of speech and expression is not absolute rather limited by reasonable restrictions under Art. 19 (2) in the interest of general public to maintain public decency and morality. Therefore, film censorship has full jurisdiction in the field of cinematograph film to prevent and control obscenity and pornography.

In Raj Kapoor v. State of Maharashtra,\(^{218}\) issue was the most controversial film, “Satyam Shivam Sundaram”. Justice Krishna Iyer held that ‘A’ certificate by a high-powered Board of Censors with specialized composition and statutory mandate is essential and acceptable. But we have to examine whether it breaches public morals and decency to invoke the penal provisions. However, certificate of the Board has evidentiary value but does not exclude criminal liability on publication of obscene and pornographic materials.

In Bobby Art International etc. v. Om Pal Singh Hoon,\(^{219}\) controversy about the film “Bandit Queen” which contains nude scene brings the Supreme Court’s attention. The story


\(^{216}\) AIR 1952 Cal 214; See also K. Jayaramanj v. Yani Karaj, 1997 Cr. L.J 1623 (Mad.)

\(^{217}\) (1970) 2 SCC 780

\(^{218}\) Raj Kapoor v. State of Maharashtra, (1980) 1 SCC 43; See also Chandra Kant Kalyan Das v. State of Maharashtra, AIR 1970 SC 1390

\(^{219}\) Bobby Art International etc. v. Ompal Singh Hoon, AIR 1996 SC 1846; See also State of Punjab v. Dina Nath, AIR 1956 Pub. 85
dealt with the life of Phoolan Devi from her childhood in village till the period of brutal torture to her. She was kidnapped, gang raped by the dacoits and was sexually harassed. The film shows how she was raped in her early age and thereafter 2 minutes nude scene in front of villagers standing around her and she was paraded nude from her head to toe. Thereafter, when she joined the dacoits group, she took revenge by killing 20 Thakur’s of her village. In that film the rapist’s obscene posterior was also shown in the rape scene. The film was based on Mala Sen’s book ‘India’s Bandit Queen’ published in 1991 and was in the market till 1994 without objection. The film was presented for certification to the Censor Board under the Cinematograph Act, 1952 and the Board allowed ‘A’ certificate with direction for some modifications. The High Court held the film as indecent and in violation of Art. 19(2), disgusting and revolting as it degraded women and those specific pornographic scenes must be deleted. However, the Supreme Court held that the film was about the real events in our society and about psychological and physical hurt to women from childhood which they are suffering in society in reality.

In Rajkapur v. Lakshman and Others,220 the Supreme Court had held that the prosecution of the producer, actor of the film, u/s 292 of the IPC was unsustainable as it had been duly certified as worthy of exhibition u/s 5-A of the Cinematograph Act, 1952.

d. Judicial Response in India after the Information Technology Act, 2000

In Jayesh S. Thakkar v. State of Maharashtra,221 the petitioners wrote a letter to the Chief Justice of the Bombay High Court, about pornographic websites on the internet. The letter was treated as *suo motu* writ petition. The Bombay High Court passed an order to appoint a committee to suggest and recommend ways of preventive and controlling measure and means to protect children from access to pornographic and obscene material on the internet.

In Air Force Bal Bharti School Case,222 a student of the Air Force Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in April 2001. The alleged accused was then a class XII student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the names of his 12 school mate girls and teachers in sexually explicit manner. He was then suspended by the School Authorities

---

220 Rajkapur v. Lakshman and Others, AIR 1980 SC 605
though the juvenile court allowed his bail prayer. However, he was charged u/s 67 of the Information Technology Act 2000, and sections 292, 293, 294 of the IPC and the Indecent Representation of Women Act.

_Tamil Nadu v. Suhas Katti_,223 was the first case of the Cyber Crime Cell Chennai. The defendant was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorcee woman. The accused at first opened a false account in the name of the victim and then sent her information through e-mails. It annoyed the victim because she had to face harrowing calls. The victim filed a complaint about the fact before police. The Chennai police traced the accused at Mumbai and arrested him immediately after few days. It was found out by the police that the accused was victim’s family friend, known to her and wanted to marry her. But she did not marry the accused. However, she married another one who ended it in divorce later on. After her divorce the accused again became very crazy about her and started contacting her but she refused for the same. Then the accused started harassing her through internet. The charge sheet was filed against the accused u/s 469 and 509 of the IPC, 1860 and section 67 of the IT Act, 2000. On the basis of the expert witness the court held that the crime is conclusively proved and the accused was convicted and sentenced to undergo rigorous imprisonment for 2 years and to pay Rs. 500 fine u/s 469 of the IPC i.e. forgery for the purpose of harming reputation; for the offence u/s 509 of the IPC i.e. word, gesture or act intended to insult the modesty of a woman with 1 year simple imprisonment and Rs. 500 fine; and for the offence u/s 67 of the IT Act, 2000 with 2 years rigorous imprisonment and Rs. 4000 fine. The court held that all these sentences must run concurrently.

In _Bhubaneswar Case_,224 the Xavier Institute of Management lodged a cyber crime complaint with the police in December 2004 that students and staff of these institutions are getting numerous obscene e-mails. Not only those, the students were afraid of online threatening, hacking and spamming. Police appointed technical experts to investigate and examine the whole technological matters. At first these indecent e-mails were considered by them as spam mails. Gradually, the students and staff were being over flooded with obscene mails and continuous sexual harassment through internet.

---

223 File No. CC No. 4680/2004/February; www.naavi.org/cl_editorial_04/suhas_katti_case.htm-9k; See also www.ceac4india.com
In Delhi Police School and Multimedia Message Service (MMS) Clip Case, a Delhi Public School boy allegedly filmed his girlfriend in an act of oral sex with him on his cell phone camera which is to be called as MMS clip. This video clip was then forwarded by him to his friends, and then his friends sent it to others. Gradually, within a minute it was available to almost all users and even it was available for small price to the roadside vendors. The clip was copied to VCD (Video Compact Disk) for sale and distribution. One IIT Kharagpur student named Ravi Raj put that MMS clip of 2.37 minutes for auction on the Baazee.com which was India’s top auction website and owned by e-Bay. The Delhi police arrested DPS student, Mr. Ravi Ray Singh and the portal’s CEO, Mr. Avnish Bajaj. The counsel for the boy contended that the charge against his client is totally false and it is very difficult to prove who was that particular person because there was no visual of his face in the clip and he prayed for bail u/s 12 of the Juvenile Justice Act, 2000 though he was arrested u/s 293, 294, 201 of the IPC, 1860 and Section 67 of the IT Act, 2000. Thus, Delhi Public School scandal was not only the issue of child pornography but also MMS clip in cyberspace.

The National Crime Record Bureau of the Home Ministry said that out of 179 cyber crime cases registered in the year 2005, 88 were related to cyber pornography; 50% of 88 cases were related to transmission of child pornographic images and video clips.

In MMS Clip of School Girl in Orkut Case, a class XII student was arrested by the cyber crime cell of the Noida police and the arrested student had confessed that he along with his friends created the picture of a girl, circulated among friends and created a fake profile of that school girl in Orkut website. He was arrested under the IPC, the Indecent Representation of Women Act and Section 67 of the IT Act, 2000. The victim girl was in clinical depression since she saw her profile in website which was posted by her school mates.

In Dr. L. Prakash Case, the accused, an orthopaedic surgeon along with his 3 staff was arrested for making cyber pornographic images of his clients forcefully and putting up

---

226Cyber Pornography on Rise, 6th October 2006, 00.52 hrs IST, Times news network
pornographic images of those women patients on the internet. The Fast Track Court sentenced accused with life imprisonment and other 3 co-accused with 7 years rigorous imprisonment.

*MMS Clip in Krishna Nagar, West Bengal Case,*\(^{229}\) a former boyfriend aged about 22 of victim was alleged to have circulated nude pictures of a first-year College girl from his mobile phone after he got married with another girl. The girl and her sister had decided not to go to University even for examinations and not to face neighbours. The entire family was in ridiculous situation that they even could not step out of house due to taunts about those pictures. Father of alleged accused was an affluent bell metal trader. He was arrested on the as victim’s father’s complaint though alleged accused was roaming freely. The Officer-in-Charge of police station said that “during their affair, accused had taken video clips on his mobile phone which he circulated among youths in the locality. He also said that the boy’s father knew and encouraged the same that was the cause of his arrest.

In *Anthony v. State of Kerala,*\(^{230}\) it was held that to be an obscene object, it need not be visible to the naked eye. Thus, the fact that the electronic impulses recorded on videotape are thrown on the screen does not make it less visible than any other visual object. Thus, the courts are found to be recognizant of changes in technology and the need to reinterpret the words.

**vi. Combatting Cyber Pornography**

New multimedia technology is being misused and abused by criminals in cyberspace. Cyber pornography, online child pornography, cyber spamming etc. are increasing every moment. Cyber pornography is not only national but also international legal challenge which needs intensive study, research and world-wide awareness.

We require more teeth to the law to cope up with the situation. We need to adopt specific and clear definition of cyber crime, cyber pornography, and child pornography in cyberspace. There is need of teaching and training to law enforcing agencies, judiciary, intermediaries, Internet Service Providers, cyber cafes, Government sectors, private sectors, teachers, students, parents and general public to be aware about effect of this dangerous threat.


to society. Banning mobile phone within the premises of educational institutions is one firm way to prevent cyber-pornography within these institutions.\footnote{Dr. Raghunath Patnaik, “Vulnerability of Children through Cyber crimes”, \textit{Central India Law Quarterly}, 2003, p. 269}

There is great need to impose more responsibilities on the Internet Service Providers and cyber cafes. They must use filter system, firewall software, regular virus scanning system and verify all detail identifications of users i.e. with photo, address, date and time of use of particular computer by particular user and the like.

Young users are very much interested to download objectionable materials and access those materials. Therefore cyber as well as parents at home must keep a watch while children are using computer. They should not use it privately.

Any person who wishes to protect their right to privacy in the cyberspace should adopt encryption process. Encryption process is a tool to cyber crime and protection of privacy in cyberspace. This is a process of self-protection or self-defense. There are 2 main key systems in encryption process and these are (i) public key and (ii) private key. When any one writes messages with encryption technique, such encryption turns that message into gibberish so that specific person to whom any one wishes to disclose or transfer his private information, that particular person only can access and read said information by using proper key of the key pair. For e.g. X wishes to send confidential information with encryption through e-mail to Z. X is confident that only Z can read the message and in it there is no likelihood of harm to that information. Here, X has to know the public key of Z. Then X will encrypt his message with Z’s public key and a programme called PGP. Then only Z can access the message by using process of decryption, sent by X to Z, by using his private key and hash function.

We can adopt the process which South Korea adopted in July 2004 making cell phone manufacturer mandatory to install a beep audible within a radius of 10 feet before using the camera mobile phone.

The situation can be curbed by the law enforcement agencies, more so police by regular track, search, seizure process, frequent visit of those suspected places to nip in the bud. With this people of India must contribute in the process of prevention and control of cyber pornography.

4. \textbf{Cyber Stalking}
i. **Historical Background of Stalking**

Stalking is quite well-known as a phenomenon surrounding celebrities. But studies show that more than 80% of victims are ‘ordinary’ people. The fact that celebrities have been stalked, and even killed by their stalkers has helped in a way......it has brought the public eye on this phenomenon. The motivations of the stalker, the effect on the stalked and the manner in which the law ought to react have all been subjects of very detailed study in the aftermath of these celebrity-stalking.\(^{232}\) Many states in the US have enacted anti-stalking legislation after these incidents as well.

ii. **Meaning of Stalking**

In very general terms, stalking refers to harassing or threatening behavior that an individual engages in repeatedly towards another person. Put slightly more crudely, it is a pattern of goal-directed behavior, both lawful and unlawful, promoted by a delusional and narcissistic perception of a relationship and intended to empower the ‘predator’ to feel omnipotent and in control, while reducing the ‘prey’s’ emotional stability to a state of vulnerability and fear.\(^{233}\)

In quasi-legal terms, \(^{234}\) stalking can be defined as a ‘willful course of conduct’ involving ‘repeated or continuing harassment of another individual’ that ‘actually causes’ the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested and that would cause a ‘reasonable person’ to feel so.

iii. **Meaning of Cyber Stalking**

The ‘Web’ is no more and no less than a mirror of the real world, and that means it also contains electronic versions of real life problems. Stalking is a problem that many people especially women, are familiar with in real life. These problems can occur on the internet as well, what has become known as ‘Cyber Stalking’ or ‘on-line harassment’. It does not end here….there have been many examples of cyber stalking crossing over to real life stalking where even physical danger is of high probability.\(^{235}\)

The fact that cyber stalking does not itself involve physical contact may create the perception that it is not as serious as physical stalking. This is not necessarily true. As the

---

\(^{232}\) In fact, the Stalking Law in the US was first enacted in reaction to the death of TV star *Rebecca Schaffer* about a decade ago.


\(^{234}\) As distinguished from the literality of a statutory definition.

internet becomes an even more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications, the Net’s intrusive capabilities, as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of internet communications may remove disincentives to cyber stalking.

iv. **Comparison between Cyber Stalking and Real World Stalking**

Research and a basic understanding of the nature of the internet show that there are some similarities as well as differences when comparing cyber stalking and real world stalking.236

a. **Major Similarities**

These are as follows:

(a). majority of cases involving stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace.

(b). most victims are women; most stalkers are men.

(c). stalkers are generally motivated by the desire to control the victim.

b. **Major Differences**

These are as follows:

(a). offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyber stalkers may be located across the street or across the country.

(b). electronic communication technologies make it much easier for a cyber stalker to encourage 3rd parties to harass or threaten a victim (e.g. impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening messages back to the victim ‘author’)

(c). electronic communication technologies also lower the barriers to harassment and threats; a cyber stalker does not need to physically confront the victim. Cyber stalking also permits the stalker to hide behind the veil of anonymity that the medium provides.

v. **Stalking Behaviour**

The acts of harassment, which manifests the stalker’s obsessions, vary widely. Some stalking begins with non-threatening letters and phone calls that express the stalker’s love for the victim. The more the victim seeks to end the correspondence, the more desperate, bizarre and dangerous the stalker’s behavior becomes. As the stalker is increasingly rebuffed, the obsession escalates, and the stalker will vacillate between deep hate for his subject and profound love and attachment. Some stalkers follow the victim, others repeatedly drives by a person’s house or workplace, still more damage the victim’s property and break into their homes and leave distinctive mark to make their presence felt. Online stalking uses the technology of the internet to achieve similar ends. Users are especially vulnerable to being targeted as cyber stalking victims in the following 3 areas:

a. **Live Chat or IRC (Internet Relay Chat)**
   A user talks live with other users. This is the most common place for cyber stalking.

b. **Message Boards and Newsgroups**
   A user interacts with others by posting messages, conversing back and forth.

c. **E-mail Boxes**
   A user has the ability to write anything and even attach files to the e-mail. Sending electronic viruses, sending unsolicited e-mail and electronic identity theft are quite common manifestations of cyber stalking.

vi. **Reasons for Stalking by a Stalker**

   Understanding what goes through a stalker’s mind could be crucial in determining the legal approach to tackling stalking of many types and also profiling a stalker’s case enables the victim to properly understand the threat perception and to take all necessary precautions.

   Traditionally, stalker’s behavior has been grouped under the following heads;

a. **Simple Obsessional**
   A prior relationship exists between the victim and the stalker which includes-acquaintance, neighbour, customer, professional relationship, lover etc.

   The stalking behavior begins after either-

   (a). the relationship has gone ‘sour’; or

   (b). the offending individual perceives some mistreatment; or

---

(c). the stalker begins a campaign either to rectify the schism or to seek some type of retribution.

This is perceived as the most common and dangerous type of stalking behaviour. Of all stalking, this type is most likely to end with harm to the victim or destruction of the victim’s property. The personality problems are what can make this type of stalker dangerous, especially if there is a history of domestic abuse. The simple obsessive stalker is likely to develop the idea, ‘if I can’t have her, then nobody else will’.
b. **Erotomanic**

A person with this delusional disorder believes that the subject of his obsession passionately loves him, even though they have never met. The erotomanic stalker pursues his subject mainly through letter writing, telephone calls, and visits to the target’s home. Even though 71% of erotomanic pursuers actually discovered their victim’s homes, few attempted to make physical contacts with their subjects. The delusion often concerns idealized romantic love and spiritual union rather than sexual attraction – “a perfect match”. The object of affection is usually of a higher status and can be a complete stranger. It may also be noted that efforts to contact the victim are common, but the stalker may keep the delusion secret.

This type of stalking behavior is perceived as not so serious and it is unlikely that any harm or damage will be caused to the person or property of the person being stalked.

c. **Love Obsessional**

There are similarities between this category of stalker and that of the erotomanic, as both types do not personally know the subject of their obsession, usually become aware of their subjects through the media, and share the goal of getting their subjects to respond to their expressions of love. The love obsessional stalker often, however, suffers from other delusional disorders, such as schizophrenia. Others suffer from no delusions; they simply love their subjects in a fanatical, obsessive way.

All of this must be seen in the context of real world stalking but the importance of knowing these is to understand the threat perception posed by each. After all, in online stalking cases it is merely a new medium for the same phenomenon.

---

238 In the overall study of stalking, the majority of victims are women and the majority of perpetrators were men, while within the erotomanic group, 86% of the pursuers were women who were obsessed with mostly male subjects (71%).

239 Supra note 19, p. 88

vii. False Victimization Syndrome

This occurs when an individual attempts to convince others that he or she is being stalked through the invention of claims made to re-establish a failing relationship or to gain attention.

This is not to be confused with situations where a stalker claims to be a victim of stalking. A notable problem with the ‘False Victimization Syndrome’ is that it wastes valuable resources. It is rare and the few cases that do occur should not undermine the reporting and investigation of legitimate stalking cases.241

viii. Stalking and the Legal Regime

Here the endeavour is to examine the present day law in India in the context of stalking in general and cyber stalking in particular. It looks at the present criminal and civil law regime and possible responsible to stalking incidents and then looks at where the loopholes lie and tries to point out why specific stalking legislation seems to make sense.

a. Stalking and Tort Law – the Civil Remedy

Tort law, through its remedy of injunctions (under the Code of Civil Procedure, 1908 for temporary injunctions and the Specific Relief Act, 1963 for other injunctions), could well be one of the remedies a victim of stalking (either real world or on-line) may have against a stalker. For an injunction to be granted it is enough to prove either damage or apprehended damage. The apprehended damage must involve imminent danger of a substantial kind or injury that will be irreparable. Specific instances when these may be got are when there is trespass, nuisance242 etc. on the part of stalker or apprehension of these.

It is also possible to bring a civil action against the stalker. This allows the victim to sue him or her for any damage they have done, for emotional harm etc. and may entitle the victim to exemplary damages and legal fees as well.

In Burnett v. George,243 the plaintiff had been subjected to a series of assaults, unwanted visits, damage to her house, telephone threats and telephone calls at unsocial hours. The Court of Appeal granted an injunction prohibiting the defendant from entering her property and from assaulting, molesting or interfering with her by acts calculated to impair her health.

241 http://onour.com/stalking/definiti.htm
242 Winfield and Jolowicz, Tort, 12th Edn. p. 380
243 (1992) 1 FLR 525
In *Khorasandijan v. Bush*,\(^244\) the tort of nuisance was utilized to grant the plaintiff an injunction against the defendant who had previously been convicted of threatening and abusive behaviour and subsequently of threatening to kill but who continued to pester her by following her and by phoning her.

In *Burris v. Azadani*,\(^245\) the law was further developed when the Court of Appeal affirmed the power of a court to include an ‘exclusion zone order’ in an injunction which restrained the defendant from, *inter alia*, “(a) assaulting, molesting, harassing, threatening, pestered or otherwise interfering with the plaintiff by doing acts to cause her harm whether directly or indirectly…. (b) making any communication to the plaintiff, whether in writing or orally…. (c) from coming or remaining within 250 yards of the plaintiff’s home address....”

The court further affirmed that the plaintiff had a cause of action in nuisance and under the tort of harassment the plaintiff had a ‘legitimate interest’ in receiving protection from behaviour ‘ which might be highly stressful and disturbing.”

While these remedies seem apt to handle stalking as a phenomenon, but the fact that they are only civil in nature carries with it the following disadvantages:

(a). they are costly

(b). it is necessary to know who the stalker is to be able to institute proceedings. This will be an enormous disadvantage as regards cyber stalking as the anonymity of the stalker is one common feature.

(c). the onus will be on the victim of the stalking to lead evidence and make out a case without the aid of the law enforcement infrastructure for investigation. This would also be at a time when he/she is undergoing the harrowing experience of being stalked. This is more so in case of cyber stalking where unless the victim is technologically aware he/she will not be in a position to make out a good stalking case with sufficient evidence of harassment in the virtual world.

(d). a power of arrest for breach of an injunction in such cases does not exist so further action on the part of the victim is necessary to institute contempt proceedings.

This is primarily why victims would normally turn to the criminal law to seek a solution to this issue.

### b. Criminal Offences

\(^{244}\) (1993) 3 WLR 476

\(^{245}\) (1995) 1 WLR 1372
While a specific offence of stalking has not been enacted in India, one may attempt to use the criminal law against stalkers. Recourse has to be taken to existing offences in the form of offences against the person and public nuisance.

c. Stalking and the Non-fatal Offences against the Person

While stalking embraces a range of conduct its impact on the victim is often to cause distress and fear. Obviously, if the stalking behaviour leads to physical attack upon the victim, a prosecution for the relevant offence against the person will be appropriate.

d. Inflicting grievous bodily harm and voluntarily causing hurt/grievous hurt

In Gelder,246 the Court of Appeal while quashing a conviction for inflicting grievous body harm contrary to the offences against the Person’s Act, 1861 arising from obscene telephone calls to the victim which has resulted in psychiatric illness, declined to consider the separate ground of appeal in which the appellant claimed that it was impossible to inflict grievous body harm over the telephone.

In Wilson,247 the House of Lords had reason to examine the meaning of ‘inflict’. The court concluded that ‘there can be an infliction of grievous bodily harm without an assault being committed. This was affirmed by Lord Mustill in Mandair.248

In Burstow,249 the Crown Court convicted the accused of inflicting grievous bodily harm on the basis of a campaign of silent telephone calls to V, hate mail, theft of clothing from her washing line and scattering of condoms in her garden. V suffered severe depression which the defence conceded amounted to grievous bodily harm and the Crown conceded that there was no assault or battery, i.e., no force was directly applied to the body of the victim. The Judge held that there was no reason for giving ‘inflict’ a narrow or restrictive meaning. In effect, ‘inflict’ meant ‘impose upon’. In response to this ruling, the accused changed his plea to guilty. This decision was affirmed by the Court of Appeal.

The Indian position with regard to stalking and hurt is slightly different. Section 319 of the IPC defines ‘hurt’ as “whoever causes bodily pain, disease or infirmity to any person is said to cause hurt.” It is obvious that if a stalker gets physically violent with the victim, a prosecution under this section could well be sustained. Stalking incidents may only leave mental and psychological scars on the victim without any sort of physical manifestation.

247 1984 AC 242
248 (1995) 1 AC 208 (229)
249 (1996) Crim LR 331
Further, clause ‘Eighthly’ of Section 320 states that “any hurt which endangers life or which causes the sufferer to be during the space of 20 days in severe bodily pain, or unable to follow his ordinary pursuit is designated as grievous hurt.” The latter part of the clause may well, in a limited way, serve our purpose. We have seen the effects of stalking and the ability of stalking incidents to have a lasting effect on victims, often making them change their lifestyles or change their jobs. This clause does provide for this in a limited sense, i.e., if the psychological effect of stalking is that the victim is unable to follow his/her ordinary pursuits for 20 days. For conviction u/s 323 and 325, the definition of ‘voluntariness’ u/s 321 and 322 have to be satisfied since a prosecution be sustained under the said sections only if there was voluntariness on the part of the accused. Section 321 states that “whoever does any act with the intention of thereby causing hurt to any person, or with the knowledge that he is likely thereby to cause hurt to any person, and does thereby cause hurt to any person, is said ‘voluntarily to cause hurt’.” There must be either intention to cause hurt or knowledge that hurt will result. Considering the wide range of stalkers, it would be very difficult to use this provision to cover this entire phenomenon. Erotomania would definitely be a case in point, the stalker being under a delusion and having absolutely no idea that what he/she is doing is causing any harm to another.

e. Assault

In the U.K., the Court of Appeal has also seen fit to rework the meaning of ‘assault’ to ensure the conviction of a stalker.

In Ireland,\textsuperscript{250} it was held that a telephone call or series of calls followed by silence could constitute an assault. In the instant case, according to psychiatric evidence ‘the victim suffered significant psychological symptoms which included palpitations, difficulty in breathing, cold sweats, anxiety, inability to sleep, dizziness and stress.’

In \textit{Fagan v. Metropolitan Police Commissioner},\textsuperscript{251} it was held that ‘assault’ in its technical sense is ‘an act by which D intentionally or recklessly causes P to apprehend immediate and unlawful personal violence’ i.e., it is apprehension of a battery and a battery is the application of unlawful force to another.

The main doubt which have existed have been as to whether words alone, unaccompanied by action, can constitute an assault. Further, there is the problem of

\textsuperscript{250} (1997) 1 All ER 112
immediacy. If force cannot be applied to the victim immediately, how can there be an assault? Clearly it is not possible to apply force over the telephone or the internet. Assault is not an offence designed to deal with the creation of fear in general. Its sphere of operation is quite narrow, namely, the creation of a fear of being subjected immediately, i.e., then and there, to a battery by the assailant. This is why it would be difficult to bring most cases of cyber stalking within the offence of assault.

In India assault u/s 351 of the IPC states “whoever makes any gesture, or any preparation intending or knowing it to be likely that such gesture or preparation will cause any person present to apprehend that he who makes that gesture or preparation is about to use criminal force to that person, is said to commit an assault.” There is little doubt that some forms of stalking behavior could very well be brought under this definition but what about cyber stalking? The first requirement is of a gesture or a preparation, the second requirement is that of ‘intending or knowing it to be likely’, the third is that the person be ‘present’ and the final requirement is that the person is ‘actually apprehensive of the use of criminal force by the accused as a result of the gesture or preparation’. The real issue is that of defining the phrase ‘person present’. Does this have to be the physical presence? One would assume so considering that the victim must have seen the ‘gesture or preparation’ as a result of which he/she is apprehensive of the application of criminal force. Thus, in the case of many stalking incidents such as obscene/blank phone calls as well as cyber stalking, this section would not apply directly, as it contemplates the presence of both the accused and the victim at the same place at the same time. The context does change a bit in the age of instantaneous communication of the telephone, the fax and the internet and their potential misuse. The IPC is a statute drafted in 1860, therefore the meaning we attribute to the word ‘presence’ need some updating, may be the virtual presence must be considered as well.

f. Public Nuisance

An offence which has recently been utilized in the UK in case of stalking is that of public nuisance.

In R v. Johnson Anthony Thomas, the Court of Appeal affirmed the conviction of the appellant of public nuisance based on his numerous obscene telephone calls over a period of 5 years to 13 different women in a particular area. The defence had contended that each of the telephone calls was a single isolated act to an individual person which could have

---

252 The Times, May 14, 1996, Cited from Allen, Supra note 14
amounted to a private nuisance but it would be wrong to treat them cumulatively to construct a public nuisance. The Court, however, decided that it was permissible to look at the cumulative effect of the calls and concluded that this amounted to conduct which ‘materially affected the reasonable comfort and convenience of a class of Her Majesty’s subjects and was a nuisance so widespread in its range or so indiscriminate in its effect that it would not be reasonable to expect one person to take proceedings on her own responsibility’.

In India, section 268 of the IPC, dealing with the offence of public nuisance is used against a stalker as well. It states that “a person is guilty of public nuisance, who does any act, or is guilty of an illegal omission, which causes any common injury, danger or annoyance to the public or to the people in general who dwell or occupy property in the vicinity or which must necessarily cause injury, obstruction, danger or annoyance to persons who may have occasion to use any public right.”

We may conclude that when the stalking phenomenon begins affecting a class of persons, this provision may be applied but it can be hardly classified as ‘the’ solution to the stalking problem. Thus, stalking, online or otherwise, ought to be controlled comprehensively with a special law, considering its potential for harm. It is in this context that many states in the US have gone in for enactment of anti-stalking laws.

g. Legal Elements of Stalking

If we need a special anti-stalking law in India along the lines of those in US, then the necessary components to make up such an offence are discussed below:

I. Course of Conduct

As many of the activities (following, watching, telephoning, sending letters or e-mails, unsolicited virtual contact etc.) which fall within the concept of stalking may be carried out with no illegitimate purpose in mind, it is important that an anti-stalking law does not unduly restrict the rights of citizens to engage in these activities. The performance of one action by a person should not be sufficient to amount to this offence. The feature that distinguishes stalking from other offences is that the stalker engages in a course of conduct in respect of the victim. To establish an offence of stalking, there should be a requirement that the stalker engages in a course of conduct comprising at least 2 separate incidents of unwanted contact. An additional requirement that the conduct be engaged in without lawful excuse would provide protection for those who may contact the victim for a legitimate purpose, albeit unwanted by him/her.
Almost all States anti-stalking laws in the US require that the defendant engage in a series of acts that, viewed collectively, present a pattern of behaviour. Some States even stipulate the requisite number of acts. \(253\)

**II. Threat requirements and Intent**

To be convicted of stalking, the stalker must also display a criminal intent to cause fear in the victim. The conduct of the stalker must be ‘willful’, ‘purposeful’, ‘intentional’ or ‘knowing’. The intent element will be met if it was reasonable for the victim to fear in the circumstances and it was proved that the accused did in fact commit the act he or she is accused of.

Thus, so long as stalking defendant knows or should know that his/her actions cause fear, the alleged stalker can be prosecuted for stalking. In this scenario, a restraining order could very well serve as a notice to the defendant that his behaviour is unwanted and that it is causing the victim to fear.

**III. Immediate Family**

A stalking defendant may, in addition to threatening the primary victim, threaten to harm members of the primary victim’s family. In a well-drafted anti-stalking law, such a threat to harm the immediate family member could be used as evidence of stalking in the prosecution for stalking of the primary victim.

**ix. Cyber Stalking – Do’s and Don’ts**

Cyber stalking is existent today and will only become more and more common as the use of computers, and the internet, increases.

Indian law has yet to come to terms with real world stalking. Talking cyber stalking seems like a distant dream.

The reception of stalking in criminal law combines two anxieties- how to determine the boundaries of acceptable social behaviour and whether to admit psychiatric damage to the front row of significant personal harms. \(254\) Indian criminal law needs to become sensitive to the issue of stalking, understand it and tackle it with an integrated societal response where not only the criminal justice infrastructure and the mental health institutions are involved but every individual understands the importance of protecting personal privacy.

\(253\) For e.g., Colorado, Illinois, Michigan, and North Carolina require the stalker to commit two or more acts on different occasions.

\(254\) Wells Celia, “Stalking; The Criminal Law Response”, 1997 Crim LR 463
a. Prevention Tips

(a). the major ‘clue’ to cyber stalking, is when the stalker pushes for information regarding your personal life, private life, or life away from the net.

(b). do not share personal information in public spaces anywhere online, nor give it to strangers, including in e-mail or chat rooms. Do not use your real name or nick name as your screen name or user ID. Pick a name that is gender and age neutral. Do not post personal information as part of any user profiles.

(c). be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.

(d). make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable user policy that prohibits cyber stalking. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.

(e). if a situation online becomes hostile, log off or surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.

(f). consider browsing the Web by going through an anonymous browsing service. This will make it impossible for your web-surfing to be logged by websites, so no one will be able to pick up any information on you.\(^\text{255}\)

(g). learn your technology. Cyber stalkers prefer to target beginners for harassment, because beginners are less likely to know what to do, and know how to fight back. Never let anyone in a chat room, or e-mail, or posting in a Usenet site, know that you might possibly be a beginner.

b. Measures to be taken if You are Being Cyber Stalked

(a). if you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.

(b). save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with internet system administrators or law enforcement officials.

(c). you may want to consider blocking or filtering messages from the harasser. Many e-mail programs such as Eudora and Microsoft Outlook have a filter feature, and

\(^{255}\) See http://www.anonymizer.com
software can be easily obtained that will automatically delete e-mails from a particular e-mail address or that contains offensive words.

(d). chat room contact can be blocked as well. Although formats differ, a common chat room command to block someone would be to type: /ignore <person’s screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the information and contact law enforcement authorities.

(e). if harassment continues after you have asked the person to stop, contact the harasser’s Internet Service Provider (ISP). Most ISP’s have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing their account. If you receive abusive e-mails, identify the domain and contact that ISP. Most ISP’s have an e-mail address such as abuse@(domain name) or postmaster@(domain name) that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint.

(f). contact the local police and inform them of the situation in as much detail as possible.

5. Cyber Defamation

i. Defamation in Cyber Space

The internet, as a global network of computers, has revolutionized the fundamental right to freedom of speech and expression. To author an article, book or poem and getting it published were the privilege of few in the pre-internet era. The multitude could never exercise their right to freedom of speech and expression in its true perspective in that era. The internet, on the other hand, is a global medium of expression. It provides limitless opportunities and ways of expression to its netizens, before a global audience. The fundamental right to freedom of speech and expression has found a global medium that is truly democratic and luxuriously easy to use. Invisibility and anonymity are significant features of internet that lend fearlessness to speech and expression. As a medium of speech and expression, the internet is equally powerful for use as well as misuse.

ii. Meaning of Defamation

256 The Constitution of India; Article 19(1) (a)
Defamation is defined as “an intentional false communication, either published or publicly spoken, that injures another’s reputation or good name.” Defamation includes the common law torts of libel (involving written or printed statements) and slander (involving oral statements). Significantly both libel as well as slander could be committed via internet medium.

iii. Ingredients of Defamation

Defamation is an intrinsically personal wrong. The gist of defamation is actual or presumed damage to reputation flowing from publication. In other words, defamation flows from publication or communication of information. In traditional libel case “publication” is generally referred to as “the date on which the libelous work was placed on sale or became generally available to the public.”

It has following ingredients:

1. Publication of a statement;
2. Statement makes reference to the plaintiff;
3. Statement is communicated to some person or persons other than the plaintiff himself;
4. Statement reaches the plaintiff; and
5. Statement causes actual or presumed damage to the plaintiff.

The question is does one encounter similar ‘ingredients’ when defamation occurs in internet medium? Here, the only difference is that the tort of defamation occurs when the defamatory imputation is published in electronic form, everything else remains the same.

iv. Various Legal Issues in Online Defamation

a. Time of Occurrence of Publication

Publication occurs when the contents of the publication, oral, spoken or written are seen and heard, and comprehended by the reader or hearer. From the point of view of plaintiff, the process of publication is complete, when the communication reaches him.

In Godfrey v. Demon Internet Ltd., the defendant ISP carried the newsgroup ‘soc.culture.thai’ and stored postings within that hierarchy for about a fortnight during which time the posting was available to be read by its customers. On 13 January, 1997 someone unknown made a posting in the US in the newsgroup. This posting was squalid, obscene and defamatory of the plaintiff who was resident in England. On 17 January, 1997 the plaintiff sent a letter by fax to the defendants, requesting them to remove the posting from their

---

260 4 All ER 342 (1999)
Usenet news server. The defendants could have obliterated the posting after receiving the plaintiff’s request, but it remained available until its expiry on or about 27 January, 1997. The plaintiff claimed damages for libel in respect of the posting after 17 January, 1997—the time when he affirmed to the ISP that the communication had indeed reached him. *Morland*, J. ruled: “In my judgment, the defendant, whenever it transmits and whenever there is transmitted from the storage of its news server a defamatory posting, publish that posting to any subscriber to its ISP who accesses the newsgroup containing that posting. Thus, every time one of the defendant’s customers accesses ‘soc.culture.thai’ and sees that posting defamatory of the plaintiff, there is a publication to that customer.”

b. **Mode of Publication**

It looks into the mode of publication or transmission - whether audio, video, textual or multimedia. Internet publishing is in ‘electronic form’. Instances of defamation in ‘electronic form’ include generating, sending or receiving ‘defamatory’ e-mails, online bulletin board messages, chat room messages, music downloads, audio files, screaming videos, digital photographs, etc. on the internet.

c. **Place of Publication and Jurisdictional Issues**

Where the publication has occurred is not easy to define as a defamatory statement can be “published” anywhere in the world where there is access to the internet. Here, the issue is whether due process of law would be served by hauling a defendant into a particular jurisdiction simply because he has posted information that can be accessed anywhere in the world.

In the context of internet, it is not necessary for the plaintiff in all cases to prove directly that the defamatory statement was brought to the actual knowledge of anyone (some person or persons other than the plaintiff himself), publication is only established if the plaintiff makes it a matter of reasonable inference that the publication was accessible in the said jurisdiction. In contrast, with the internet it is not at all probable that every website will be accessed in every jurisdiction where it can theoretically be accessed. So, as a matter of reasonable inference, it cannot be assumed that any site put on the internet and theoretically accessible from anywhere is in fact accessed everywhere.261

---

In *R v. Graham Waddon*, the defendant was charged with numerous counts of publishing obscene articles contrary to Section 2(1) of UK’s Obscene Publications Act, 1959. The defendant had created pornographic images, which were illegal under the UK’s Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US based Internet Service Provider. These images were accessible to anyone in the world via the internet who became a subscriber by giving credit card details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images. It was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore the instant court did not have jurisdiction. *Hardy Christopher*, J. held: “Publishing an article under Section 1(3) (b) of the 1959 Act included data stored electronically and transmitted. To transmit simply meant to send from one place or person to another. In the instant case, an act of publication took place when the data was transmitted by the defendant or his agent to the service provider, and the publication or transmission was in effect still taking place when the data was received. Both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving”.

In *Dow Jones & Company Inc v. Gutnick*, an alleged defamatory article appeared in *Barron’s Online*, the online version of Dow Jones’s print publication *Barron’s*, which was available to subscribers of wsj.com. Joseph Gutnick, a resident of the Australian state of Victoria, brought a defamation action against Dow Jones in a Victoria Court. Dow Jones argued that *Barron’s Online* was published in New Jersey, the location of the servers hosting the wsj.com website. From this it would follow that the substantive law to be applied in deciding the case is New Jersey law, which would make the Victorian Court a clearly inappropriate forum. The Court held that the article was published, with respect to Gutnick’s cause of action, not when Dow Jones placed it on its web server, but only when subscribers in Victoria accessed it. Thus, the defamation occurred in Victoria, and that Victorian law governed. The court concluded for centuries that the law in defamation cases has been that publication takes place when and where the contents of the publication, oral or spoken, are seen and heard, and comprehended by the reader or hearer. Having decided that a person is

---

262 Southwark (Crown Court, 30/6/1999)
263 [2002] HCA 56 (Austl.)
defamed at the place where publication is made, the court found that the dissemination of the material on the internet and the downloading of that information in Victoria meant that publication had been made there.\textsuperscript{264}

In \textit{Joseph Gutnick v. Dow Jones & Company Inc.},\textsuperscript{265} the Victorian Supreme Court held that the “publication” of an online article occurred in the jurisdiction where the article was downloaded, regardless of where it was uploaded or where the publisher’s server resided. Subscribers downloaded and paid for the article through a Victorian Web browser and the meaning of the article was conveyed to the reader in Victoria. For these reasons, plaintiff succeeded in establishing that Victoria was the relevant jurisdiction. This judgment has made it clear that a person is defamed at the place where publication is made, and in the context of internet it is the downloading of the information that is a relevant fact for identifying the jurisdiction. The criticism that the plaintiffs may resort to “forum shopping” in order to bring their claim in a jurisdiction which provides them with a greater chance of success is untenable. Before deciding any case, the courts will have to observe whether there exists a substantial connection with the place where proceedings are instituted.

d. Liability of Internet Service Provider (ISP) or Website Promoter for Publication

An Internet service provider represents an interactive network service. It may provide access to the internet only or offer a range of additional services. Depending upon its functional attributes, an Internet service provider may act as an ‘information distributor’ or ‘information publisher’. An ‘information distributor’ merely acts as a carrier of information, transmitting ‘electronic message’ from one place to another, without examining its content. The function of an ‘information publisher’ is to not only publish and transmit the information but also take reasonable care in relation to the said publication.

In \textit{Cubby, Inc. v. CompuServe, Inc.},\textsuperscript{266} where CompuServe is an online company providing access to over 150 special interest forums comprised of electronic bulletin boards, interactive online conferences, and topical databases. A newsletter called \textit{Rumorville} was made available \textit{via} the bulletin board. The plaintiff sued CompuServe for libel after allegedly defamatory statements were disseminated through the newsletter against it. Cubby argued that the court should consider CompuServe to be a “publisher” of the allegedly defamatory statements, and thus hold it liable for the statement. The court held that CompuServe had “no

\begin{itemize}
\item \textsuperscript{264} \textit{Yahoo v. LICRA}, 168 F Supp. 3d 108 (N.D. Cal. 2008)
\item \textsuperscript{265} [2001] VSC 305
\item \textsuperscript{266} 776 F. Supp. 135 (S.D.N.Y. 1991)
\end{itemize}
more editorial control over such a publication than does a public library, bookstore, or
newsstand.” The court instead found CompuServe to be more akin to a “distributor” rather
than a “publisher.” Thus, because it was undisputed that CompuServe did not have
knowledge of or reason to know of the allegedly defamatory statements made in the
publication, especially given the large number of publications it carries and the speed with
which publications are uploaded into its computer banks and made available to CompuServe
subscribers, the Court held that CompuServe could not be held liable to Cubby for the
defamatory statements. The Court noted that to impose on CompuServe the duty to examine
every publication it carries for defamatory statements would “impose an undue burden on the
free flow of information”.

In Stratton Oakmont, Inc. v. Prodigy Servs. Co., plaintiffs, a securities investment
banking firm sued Prodigy Services Company, an interactive computer service, for
defamatory comments made by an unidentified party on one of Prodigy’s bulletin boards
against the firm. The court held Prodigy to the strict liability standard normally applied to
original publishers of defamatory statements, rejecting Prodigy’s claims that it should be
held only to the lower “knowledge” standard usually reserved for distributors. The Court
reasoned that Prodigy acted more like an original publisher than a distributor, both because it
advertised its practice of controlling content on its service and because it actively screened
and edited messages posted on its bulletin boards using customized software.

v. Online Defamation Laws and Judicial Approach in Various Countries

a. Position in U.S.

The US Congress enacted the Communication Decency Act, in 1996, not to treat
providers of interactive computer services like other information providers such as
newspapers, magazines or television and radio stations, all of which may be held liable for
publishing or distributing obscene or defamatory material written or prepared by others. It
opted not to hold interactive computer services liable for their failure to edit, withhold or
restrict access to offensive material disseminated through their medium. The statutory
emphasis has been to protect and strengthen the ISPs business model.

The Communication Decency Act of 1996 provides:

---

“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

Any person who puts information on the web which is obscene, lewd, lascivious, filthy or indecent, with intent to annoy, abuse, threaten, or harass another person, will be punished either with imprisonment or with fine. As for as civil liability is concerned no provider or user of an interactive computer service shall be held liable on account of:

(i) Any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or

(ii) Any action taken to enable or make available to information content providers or others the technical means to restrict access to materials described above.

The term “interactive computer service” means “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provide access to the internet and such systems operated or services offered by libraries or educational institutions.”

The term “information content provider” is defined as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the internet or any other interactive computer service.”

In Zeran v. America Online Inc., on April 25, 1995 an unidentified person posted a message on an American Online (“AOL”) bulletin board advertising “Naughty Oklahoma T-Shirts”. The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995 bombing of the federal building in Oklahoma City. Those interested in purchasing the shirts were instructed to call “Ken” at Kenneth Zeran’s phone number in Seattle, Washington. As a result of this prank, Zeran received a high volume of phone calls, comprised primarily of angry and derogatory messages and death threats. He informed and requested AOL to remove the offensive message from its bulletin board, but of no avail. Zeran consequently brought an action against AOL and argued the AOL

---

268 The Communication Decency Act, 1996; Section 230(c) (1)
269 Ibid.; Section 223
270 Ibid.; Section 230 (c) (2)
271 Ibid.; Section 230 (e) (2)
272 Ibid.; Section 230 (e) (3)
273 129 F.3d 327 (4th Cir. 1997)
unreasonably delayed in removing the defamatory messages posted by the unidentified person and failed to screen for similar postings thereafter. In an attempt to circumvent the protections afforded to an “Interactive Computer Service” under section 230(e)(2) of the CDA the plaintiff argued that AOL’s knowledge of the defamatory nature of the posting exposed it to liability as a distributor and therefore placed it outside the ambit of the CDA’s protections. The Fourth Circuit rejected this argument, and held that under section 230 of the CDA, AOL is immune from liability for the information that originated with a third party. The Court observed that the purpose of section 230 is evident: “interactive computer services (such as AOL) have millions of users. The amount of information communicated via interactive computer services is, therefore, staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems”.

In *Lunney v. Prodigy Services Company*,274 an imposter opened a number of accounts with Prodigy Services Company, an ISP, and proceeded to post two vulgar messages in Lunney’s name on a Prodigy bulletin board and send a profane electronic mail (e-mail) in Lunney’s name to a third party. Lunney sued Prodigy for defamation and negligence. With respect to the e-mail message, the Court found that because Prodigy was only a conduit for the message, and it did not exercise influence or control over the content of the transmitted communication, it should be given the same privilege accorded to telephone and telegraph companies. With respect to the bulletin board message, the Court concluded that while Prodigy does reserve the right to screen its bulletin board messages, this would not alter its passive character in “the millions of other messages in whose transmissions it did not participate”. Thus, the Court refused to cast an electronic bulletin board operator, such as Prodigy, in the role of a publisher.

In *Schneider v. Amazon.com Inc.*,275 an author sued Amazon.com for defamation and tortious interference with a business expectancy, based on a negative and allegedly defamatory book review posted by a third party. The plaintiff argued that Amazon.com was not a provider of an “interactive computer service,” since it did not enable access to the internet: to visit the site, a user must already be online through some other service provider. The Court rejected plaintiff’s argument explaining that Amazon’s website postings appear

275 31 P.3d 37 (Wash. Ct. App. 2001)
indistinguishable from AOL’s message board (in Zeran v. America Online) for section 230 purposes. Amazon’s web site enables visitors to the site to comment about author and their work, thus providing an information service and hence could be referred as an interactive computer service under section 230 (e) (2) of the CDA.

In Doe v. America Online, Inc.,276 mother’s action on behalf of her son against AOL, an interactive computer service provider, arising out of user’s alleged sale of obscene material involving mother’s son on the Internet, the CDA protected AOL from liability even though mother sought to hold AOL liable as a distributor of child pornography rather than as publisher or speaker.

In Ben Ezra Weinsten v. America Online, Inc.,277 operator of interactive computer service was immune under the CDA against negligence and defamation claims of corporation for which allegedly inaccurate stock information was provided on service. The U.S. Court of Appeals for the Tenth Circuit affirmed the U.S. District Court’s opinion by ruling that America online acted solely as an interactive computer service provider when it provided access to allegedly inaccurate information regarding Ben Ezra, Weinsten’s publicly traded stock and, therefore, is immune from suit under Section 230 of the CDA.

Blumenthal v. Drudge,278 CDA barred imposing liability on AOL, which merely made defamatory gossip column available to its subscribers, in absence of evidence that AOL had some role in writing or editing material, or creating or developing information in column.

In New York Times v. Sullivan,279 I was held that in US the ‘public figure doctrine’ requires that the plaintiff in a defamatory action must prove actual malice on the part of the publisher to succeed in an action for defamation.

b. Position in U.K.

The U.K. Defamation Act, 1996 contains an “innocent dissemination” defense which is available only if the defendant took “reasonable care” and “did not know, and has no reason to believe” that he was publishing a defamatory statement.280

The Defamation Act, 1996 provides:

In defamation proceedings a person has a defense if he shows that-

---

276 718 So.2d 385 (Fl. App. Ct. 1998)
277 206 F.3d 980 (10th Cir. 2000)
279 198 F Supp. 815 (N. D. NY. 1964)
280 Emmens v. Pottle, (1885) 16 QBD 354, 357; See also Vizetelly v. Mudie’s Select Library Ltd., (1900) 2 QB 170,179
(a) he was not the author, editor or publisher of the statement complained of;
(b) he took reasonable care in relation to its publication, and
(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.281

For this purpose ‘author’, ‘editor’ and ‘publisher’ have the following meanings: ‘author’ means the originator of the statement, but does not include a person who did not intend that his statement be published at all; ‘editor’ means a person having editorial or equivalent responsibility for the content of the statement or the decision to publish it; and ‘publisher’ as a commercial publisher, that is, a person whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business.282

A person shall not be considered the author, editor or publisher of a statement if he is only involved in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form.283

In determining whether a person took reasonable care, or had reason to believe that what he did caused or contributed to the publication of the defamatory statement, regard shall be had to-

(a) the extent of his responsibility for the content of statement or the decision to publish it;
(b) the nature or circumstances of the publication; and
(c) the previous conduct or character of the author, editor or publisher.284

Presumably the U.K. Defamation Act, 1996 offer some protection to ISPs, and there is evidence in the legislative record that the Govt. intended ISP to fall under section 1 (3).285

c. Position in Canada

281 The Defamation Act, 1996; Section 1(1); See also L. Dolding and S. Dzioban, “Electronic Communication and the Defamation Act, 1996: Clarity or Confusion?” (1997) 6 Information and Communication Technology Law Rev 55
282 Ibid.; Section 1(2)
283 Ibid.; Section 1(3) (c)
284 Ibid.; Section 1(5)
As with other Commonwealth countries, Canada also follows United Kingdom law on defamation issues. Recently the Supreme Court of Canada in the case, *Hill v. Church of Scientology of Toronto*,\(^2\) has reviewed the relationship of the common law of libel and its relation to the Canadian Charter of Rights and Freedoms.

### d. Online Defamation: An Indian Perspective

In India, issue of defamation has so far been dealt under the provisions [Ss.499-502] of the Indian Penal Code, 1860. The Code makes no distinction between a slander and a libel. It defines “defamation” as: “Whoever by words, either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the case hereinafter excepted, to defame that person.”\(^3\)

The main three ingredients of defamation\(^4\) are:

a. Making or publishing any imputation concerning any person

b. Such imputation must have been made by

   (i) Words, either spoken or intended to be read; or 
   (ii) Signs; or
   (iii) Visible representations

c. Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.\(^5\)

The Code also prescribes the punishment for defamation as: “Whoever defames another shall be punished with simple imprisonment for a term, which may extend to two years, or with fine, or with both”.\(^6\)

In *Amar Singh v. Budalia K.S.*,\(^7\) it was held that the criminal liability for defamation u/s 499 of IPC rests on the ‘maker or speaker or author’ and the ‘publisher’ of the defamatory content. The words ‘maker or speaker or author’ do not present any difficulty or doubt. The key word in sec. 499 is ‘publishes’. In simple terms, the making known of the defamatory

\(^2\) (1995) 20 DLR (4th) 190

\(^3\) The Indian Penal Code, 1860; Section 499

\(^4\) Ratanlal & Dhirajlal, *The Indian Penal Code*, 28th Edn., p.686

\(^5\) *Id.* at p. 687; See also P.A.S. Pati, “Applicability of I.P.C. to Cases of Cyber Crime”, available at http://www.naavi.com/pati/cybercrime2.html, visited on May 12, 2010

\(^6\) Supra note 283, Section 500

\(^7\) (1965) 2 Cr.L.J. 6593 (Pat)
matter after it has been authored to some person other than the person of whom it is written, is publication in the legal sense.

In *Bennett Coleman & Co. v Union of India*, the Supreme Court held that “publication means dissemination and circulation”. That is, communicating defamatory statements only to the person defamed is not publication.

It is important to note that an essential difference between the Indian and the English law is that the former recognizes ‘words spoken’ as a mode of defamation, and the latter does not.

In *Balraj Khanna v. Moti Ram*, it was held by the Supreme Court that “it will be highly desirable no doubt if the actual words stated to have been used by an accused and which are all to be defamatory are reproduced by the complainant. The actual words used or the statements made may be reproduced verbatim by the complainant if the words are few and the statement is very brief. But in cases where the words spoken are too many or the statements made are too long, it will be the height of technicality to insist that the actual words and the entire statements should be produced verbatim.”

The Code by highlighting that defamation could also happen by means of ‘signs’ or ‘visible representations’ has included every possible form of defamation, including defamation in ‘electronic form’ as well. Instance of defamation in ‘electronic form’ includes generating, sending or receiving ‘defamatory’ e-mails, online bulletin boards messages, chat room messages, music downloads, audio files, screaming videos, digital photographs etc. on the Internet. Even sending ‘defamatory’ SMS, MMS, photographs and videos on mobile phones would be considered instances of defamation in electronic form. In other words, the Code is sufficient in itself to tackle any online defamation matter.

The Information Technology Act, 2000 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to 2 years and with fine which may extend to Rs. 25000 on first conviction and in the event of second conviction, the imprisonment may extend to 5 years and fine may extend to Rs. 50000, but it does not expressly talk of cyber defamation.

---

292 (1972) 2 SCC 788
294 AIR 1971 SC 1389
295 The Information Technology Act, 2000; Section 67
Issue of Jurisdiction

A claim for damage to reputation will warrant an award of damages only if the plaintiff has a reputation in the place where the publication is made. This has always been the accepted legal principle in the common law countries. In India, the same principal has been adopted—publication takes place when and where the contents of the publication, oral, spoken or written are seen and heard, and comprehended by the reader or hearer.

In *P. Lankesh v. H. Shivappa*, it was held that where a newspaper containing a defamatory article is published at one place and is circulated or sold at other places by or on behalf of the accused responsible for printing and publishing the newspaper, then there would be publication of the defamatory article in all such places........if the defamatory imputation is made available to public at several places, then the offence is committed at each such place.

Extending the aforesaid principle in the Internet environment, a publication would take place where the information is downloaded which means retrieving a file (digital content) from a remote computer, computer system or computer network. It is a software driven process that requires accessing an Internet Service Provider (information distributor or publisher) and submitting to the web browser a ‘downloading request’ in the form of a ‘uniform resource locator’ (URL). Once a website is download, one may again select any of the links present for further downloads. The publication occurs when the downloading is complete (or done) at the user’s end. Thus, any time a user accesses and sees (downloads) defamatory information of the plaintiff, there is a publication to that user.

It is obligatory that before declaring whether an online ‘publisher’ or ‘distributor’ is liable for defamation under the aforesaid provisions of the IPC, one should also take cognizance of the Information Technology Act, 2000. The said section expresses the legislative intent of granting immunity to the network service provider. The immunity is absolute—if and only if he proves for any third party information that:

(i) he had no knowledge that the information content it is transmitting is unlawful; or

(ii) he had exercised all due diligence to prevent transmission (or publication) of unlawful information content.

---

296 1994 Cr. L. J. 3510 (Kant)
297 Supra note 291, Section 79
A “network service provider” may act as an online ‘publisher’ or ‘distributor’, though no such categories have been identified in the information Technology Act, 2000. In that way, the Indian position is closer to the English law [S 1 (1) (b)] and S. 1 (1) (c) of the Defamation Act, 1996] than to the US, Communication Decency Act, 1996 [47 USC 230] which forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self regulatory functions.

vi. Factors to be taken into Consideration for Determining Liability in Online Defamation

ISPs and website hosts or owners must therefore take care to control, as far as possible, the information published on their websites. Factors which could possibly be taken into account in determining whether an ISP or a website host/owner have exercised reasonable care are as follows:298

a. The nature and purpose of the site containing the defamatory material and the relationship of the defendant thereto, that is, whether the defendant is bulletin board operator or an ISP or simply a company controlling its own website;
b. Whether the monitoring system which was put into place is proportionate to the size of the site;
c. The amount and characteristics of information flowing through the site;
d. The characteristics of the site users;
e. Whether or not the site attracted repeat offenders and, if so, why the site was then not removed;
f. Whether defamatory materials is removed immediately upon request by the person being defamed.
g. Measures which would assist in reducing the exposure of an ISP or website host/owner to liability for defamation include:
h. The posting of clear notices warning potential users of the site not to put libelous material onto the site;
i. Periodic monitoring of sites and bulletin boards with a view to the deletion of any problematic material;

---
j. The introduction of systems to facilitate the speedy publication of apologies in respect of any statements published on the site which are found to contain libelous allegations;

k. Making access to the site conditional upon the provision by any user of its name, address and other specified identifying data so that the author of any defamatory statement may later be traced and disclosed to a potential defendant if a claim for defamation is threatened.

vii. Combating Cyber Defamation

The law regulating the various facets of Internet usage is still very much in an embryonic phase. There is no way that the law can keep up with the pace at which technology is developing. We are, however, certain of one thing and that is that the scope of every cyber consumer’s exposure to liability for defamation is global. The present trend of legislation and also the judicial approach to such offences appears to be such that these offences are treated lightly and the punishments are not adequate having regard to the gravity of such offences. Therefore, the need of hour is that the Government should take up the brave task of analyzing such crimes, which are at the threshold, and come up with recommendations in order to equip the existing legal machinery against such offences. For the said purpose, necessary amendments could be brought to Section 67 of the Information Technology Act, 2000 and also to Section 499 of the Indian Penal Code, by expressly bringing within their ambit offences such as defamation in cyber space, which is certainly a socio-economic offence.

6. Cyber Terrorism

i. Historical Background of Cyber Terrorism

Terrorism is a kind of threat or terror against common people or Government which is not predictable. 11th September, 2001 attack on World Trade Centre and Pentagon in the USA; 7th July 2005 attack in London; attack in Mumbai in 2006, defacement of Indian Military sites in India by hackers in July 2005, etc. are few examples of terrorist attack.

According to the Symbolic Communication theorist P.K. Kraber “as a symbolic act, terrorism can by analyzed much like other media of communication consisting of 4 basic components- transmitter, intended recipient or receiver who are, message bombing, explosives and feedback reaction of targeted audience.”

According to Garbriel Weimann, “modern terrorism may be construed as an attempt to communicate messages through the use of orchestrated violence.”

**ii. Concept of Cyber Terrorism**

The term ‘Cyber Terrorism’ is coined by a senior research fellow in California Institute for Security and Intelligence, Mr. Barry Collin in 1980s who says that it is composed of 2 terms namely ‘cyberspace’ and ‘terrorism’. According to him “Cyberspace” is the place where computer data move and computer functions. The United States Code defines the term “Terrorism” as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience. Further, “Information Terrorism” is “the intentional abuse of a digital information system, network or component towards an end that supports or facilitates a terrorist campaign or action.

There are 2 prime concepts of Cyber Terrorism - (1) When terrorists use information technology to attract their audience by creating violence, through defacement of web site, denial of service attack, hacking, cracking, tampering source code, flowing viruses etc. where computer is used a target or weapon and which go against Government or national security, (2) Another is terrorized use of IT i.e. cyber pornography, cyber fraud, cyber theft, spamming etc. which causes terror or threat in the mind of people.

Internet has no boundary and it is not possible to define definite jurisdiction in cyber space. Therefore, terrorist groups are increasing day by day and they can easily access one another even living in different countries. For e.g. Al-Qaida group, Jihad group and other terrorist groups have spread worldwide and connecting each other through World Wide Web and communication convergence technology.

**iii. National Security**

National security of a nation depends on the following:

**a. Confidentiality**

Confidential information of a nation are those losses which will cause loss to national security.

---

302 The United States Code; Title 22 Section 2656 f (d).
303 Ibid.
b. **Secret information**

Secret information of the nation are those losses which will cause more grievous losses to the security of the nation than loss of confidentiality.

c. **More secret information**

More secret information of the nation are those losses which will cause more grievous damage or extreme injuries.

Therefore, confidentiality, secrecy and more secrecy are to be treated as the key to maintain national security. When terrorists attack on those keys through cyber world or within cyber world, they commit cyber crime which is called cyber terrorism.  

---

iv. **Modes of Cyber Terrorism**

a. **Cyber terrorism is the forerunner of warfare**

In the era of information and communication technology (ICT) one nation causes terrorist violence by using new technology against other nation or nations. These are not the conventional way of war rather cyber war or net war between 2 or more nations which are very much unpredictable. For e.g. net war between Israel and Pakistan, India and Pakistan, China and USA.

b. **International cyber terrorist attack**

When International Organizations of terrorists link or communicate between them through internet and attack any nation, it is called international cyber terrorist attack. For e.g. 11th September 2001 attack on World Trade Centre and Pentagon; immediately after that 13th December 2001 attack at Indian Parliament.

c. **Use of computer system and internet facilities**

Use of computer system and Internet facilities by terrorists group to develop own websites and network to send messages to each other worldwide are effective mode of cyber terrorism.

d. **Cyber terrorists use encryption programme and digital signature**

Cyber Terrorists use encryption programme and digital signature to coordinate themselves using e-mail service which cannot be read by any one. Even the National Security Agency through their super computing system failed to crack terrorist group’s code. The USA is fighting against these attacks since 1990s.

e. **Terrorists now using Information and Communication Technology (ICT) including satellite transmission**

Terrorists now use ICT including satellite transmission, cell phones, wireless etc. to communicate with each other and organize for terrorist attack.

f. **Flowing ‘worm’, ‘virus’, ‘Trojan horse’**

Flowing ‘worm’, ‘virus’, ‘Trojan horse’ etc. are used to collapse Government departments such as defence, intelligence, commerce, academic and health. Access to Global electronic network and information is one way which facilitates cyber terrorism.

v. **Evolution of Cyber Terrorism**

---

Cyber terrorism can be traced from June 1944 attack on the communication lines and logistic support of Germany.

In 1986 West German hackers’ accessed departments of defence of the USA which was an example of cyber terrorism.

In 1988 Osama Bin Laden established Al-Qaida as Islamic resistance movement against the Soviet forces in Afghanistan. This name was coined by the U.S. Government from a computer file where Laden listed the name of contact he had made in Afghanistan and where he expressed the organization as Qaida-al-Jihad which is based on Jihad. As presumed they attacked on the USA in 1998, 2000 and 2001 as well as on the UK on 7th July, 2005 and thereafter.

Gradually information warfare or net was speeded worldwide. Gulf war was the first information war through Information-Way (I-Way). In mid 1990s the USA started investing more on national security, infrastructure and to strengthen themselves for information war. Even they had started employing hackers or ‘I-Way gurus’ to achieve the goal. The USA passed the Nation Infrastructure Protection Act, 1996.

By 1998, all over the Europe, more countries had started initiatives to fight against it. In the UK, the Defence Evaluation and Research Agency was established in 1998 following the US Defence Intelligence Agency. Even Germany, France and other countries came forward to combat cyber war almost in the same ways.

In India, LTTE group’s works depend mostly on network, websites and internet connectivity. Aftab Ansari’s attack on American Centre, Kolkata was based on their organization through internet and websites. Even from Dubai he was able to communicate with his group. Therefore, in the contemporary communication convergence era cyber terrorism has become the most complex and national as well as an international problem. There is great need of co-operation and co-ordination between all States in the era of globalization and liberalization.

vi. **International Initiatives to Prevent and Control Cyber Terrorism**

Cyber terrorism brought back the cold war situation again. The United Nations and European Union always played and are playing significant roles to prevent and control the menace.

a. **International Ministerial Conference**

In July 1997, the International Ministerial Conference on global information networks was held in Bonn. This conference brought every Member State under one umbrella of information and communication technology. World Wide Web users, International Organizations and IT Industries came together for the protection of net users and to evolve standards of functioning systems and self-regulations.

b. **The Justice and Home Affairs Council**

The Justice and Home Affairs Council also came forward to establish practical cooperation between counties worldwide at the investigative and procedural stages. For this end the G-8 Senior Level Group on the transnational organized crime was investigating mechanisms to determine, identify and prosecute cyber terrorism and other computer-related crimes. In April 1997, the European Commission and the European Police Forces took initiatives to control illegal content on the internet, reporting, investigating cross border links, exchange of information, to reconcile national laws and to co-operate investigations.

c. **The News Conference of the G-8 Countries**

G-8 countries are the largest group of industrialized countries in the world. In December 1997, G-8 Conference was held at FBI headquarter. The US Attorney General Janet Reno said “Criminals no longer are restricted by national boundaries….If we are to keep up with cyber crimes, we must work together as never before.” The news conference released their report for the following areas where these major nations have agreed to collaborate:

(a). To assign number of properly trained and equipped law enforcement personnel to investigate high tech crimes;

(b). To improve ways to control attacks on computer networks;

---

309 Ibid.
c. To prosecute criminals in the country where they are found, when extradition is impossible;

d. To preserve key evidence on computer networks;

e. To review the legal codes in each nation to ensure that appropriate crimes for computer wrong doing are prescribed;

f. To ensure that the language makes it easier to investigate the crimes;

g. For cooperation with the private sector to develop new ways to detect and prevent computer crimes;

h. To increase efforts to use new communication technologies, such as video teleconferencing to obtain testimony from witnesses in other nations.

d. European Committee on Crime Problems

On 22nd December 2000, the European Committee on Crime Problems and Committee of Experts on Crime in Cyber space adopted a draft Convention on cyber crimes with due regards to:

(a). Common criminal policy for the protection of society against cyber crimes,

(b). Globalization, digitalization and convergence of computer networks,

(c). Preservation of evidence in computer network,

(d). International cooperation to combat cyber crime,

(e). To adopt necessary measures to deter activities against confidentially, integrity and availability of computer system, networks and data,

(f). To adopt necessary measures to deter against computer misuse to control cyber crimes,

(g). To achieve above objectives every member state has to facilitate detection, investigation and prosecution of cyber crimes at national and international level,

(h). To ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as established by the European Council’s Convention for the Protection of Human Rights and Fundamental Freedoms and in 1966 the United Nations International Convention on Civil and Political Rights.
vii. The United Kingdom’s Initiatives to fight against Cyber Terrorism

The Terrorism Act, 2000 defines the term ‘terrorism’ as “the use or threat of action that is designed seriously:

(a) To interfere with or seriously to disrupt an electronic system,
(b) To influence the government or to intimidate the public or a section of public, and
(c) For the purpose of advancing a religious, ideological or political cause.”

In 1970, politically-motivated crimes were in rising mode in the UK. Anti-Terrorist Branch was formed in 1976. There were also rise of threats and attacks to the government, government agencies, departments and people through superhighway using information technology. Therefore, the UK enacted the Data Protection Act, 1984 and in 1990 to prevent and control cyber terrorism and other crimes the Computer Misuse Act was enacted and passed after R. v. Gold. The Computer Misuse Act, 1990 prohibits cyber hacking, following viruses, worm, objectionable materials, cyber fraud and other cyber crimes. When these crimes are committed with intent to cause damage to general people and government by causing threat or apprehension of danger or terror then these crimes are to be treated as cyber terrorism.

In December 2004, news was published in internet and TV channels worldwide that diplomatic missions and military forces of the UK will be the prime target of terrorists attack. The attacks will be same as was in November 2003 on the British Consulate in Istanbul; in September 2004 on the Australian Embassy in Jakarta; on the US Consulate in Jeddah in December 2004. Terrorists accessed internet as weapons to threaten through most of the websites.

On 11th March 2004, terrorists attacked on commuter trains in Madrid. A London based newspaper reported about receiving of an e-mail from a terrorist group affiliated with Al-Qaida and videotape claiming responsibility of the said attack. Al-Qaida is running several websites such as Alneda.com, Jehad.net to run their terrorist activities in easiest way.

Attack on a vehicle in Yemen in 2002 was new form of high-tech warfare by distant operators through computer screens in the same way as Al-Qaida attachk on the USA on 11th September 2001.  

311 (1988)1 1060; see also [1987] WLR 803
A letter containing ‘Terror Hits London’ was left in internet with the help of a deadly Trojan virus and an online CNN news letter containing exclusive video footage on the terrorist attack after 7th July 2005 incidents of London blasts. It invites recipients to see the attachment and video shots. At the moment users started downloading, it started coping users system, accessed mail servers and others and started sending spam. More than 53,000 computers were infected by this Bo-box worms which contained Bin Laden or Saddam Hussein pictures.

viii. United States Initiatives to Prevent and Control Cyber Terrorism

After 11th September 2001 attack on World Trade Centre and Pentagon, the USA passed the Patriot Act, 2001 and recognized hacking as cyber terrorism. The Computer Fraud and Misuse Act, 1986 was amended to prevent and control computer misuse by terrorists and terrorized use of computer.

The U.S. Code provides that where with intention or with knowledge any one or group or groups access without authority any protected computer or computers which are recognized and determined by the Government by executive order or statute as protective computer or computer system to protect (i) national defence, or (ii) foreign relation, or (iii) any restricted data with reasonable belief that any unauthorized access which may cause injury to the United States or foreign nation’s interest’ commits an offence. He will be punished with 10 years imprisonment or with fine or with both for the first time committed offence and for crime committed by a convict with 20 years imprisonment or with fine or with both. Further, it prohibits unauthorized access or access exceeding authorization to obtain information of financial institution, information from any one of the US agencies or department, information from any protected computer involved with interstate or foreign communication. This is punishable with 5 years imprisonment or with fine or with both when it is committed for violation of Constitution or other laws of the U.S.A. for first time offence and with 10 years imprisonment or with fine or with both for crime committed by convicted person or by habitual offenders.
United States v. Raymond Torricell, the defendant was the head of a hacker group known as ‘#conflict’. He was arrested at his home in New York City for allegedly breaking into 2 computers owned and maintained by the National Aeronautics and Space Administration’s (NASA) Jet Propulsion Laboratory (JPL) in California and for using one of those computers to host an internet chat-room devoted by him for hacking. The defendant unauthorizedly accessed a computer for spamming by which process he used to send unsolicited advertisements over the internet to large numbers of computer users, promoted a pornographic website, intercepted passwords, unauthorizedly used the name of the computer network maintained by Georgia Southern University. He was also charged for password theft and decryption of password. After gaining control over NASA’s first computer he installed a programme to enable chat room discussion with members of ‘#conflict’ and to commit other crimes. Thereafter, he controlled NASA’s 2nd computer and installed a sniffer programme for interception of user names and password. He thus decrypted over 76,000 passwords, gained unauthorized access over 800 computers and earned about $ 300 to 400 per week only from spamming. He was charged under US Code Title 18 section 1030, and punished with 4 months imprisonment, 4 months confinement and to pay $ 4,400 in restitution to NASA with others.

a. The Patriot Act, 2001

11th September, 2001 was ‘Cyber Terrorist Attack’ in new uncertain information technology and internet dominated world. Therefore, in October 2001 the Patriot Act was passed by the United States Congress which recognized that those who break into others computer, commit hacking, cracking and other cyber crimes which cause loss of National interest could be considered as cyber terrorists and must be prosecuted.

b. United States is Signatory to the Convention on Cyber Crime

In November 2001, the US signed the Convention on Cyber Crime which was the first international, multilateral treaty which specifically asks all the member states for international cooperation in the investigation and prosecution of cyber criminals; which includes extradition of criminals, searches and seizures, prosecutions with substantive and procedural provisions.

c. Cyber Security Enhancement Act, 2002

---

The US passed the Cyber Security Enhancement Act in 2002 to prevent and control cyber terrorism and other cyber crimes and to implement security measures.

In *United States v. Dino A. Amato*, the defendant was a former contract employee of computer service at the NASA. When he was in employment, he downloaded ‘zipped’ computer file called ‘zip-42’ from the internet. He then transmitted the same through internet to an e-mail account holder of NASA e-mail server more than 7 times with intention to cause damage of about $12,000. He was charged for the violation of Title 18, U.S.C. Section 799 and for violating NASA’s rules and regulation. He was also punished with 1 year imprisonment and $100,000 fine.

In *United States v. Racine*, the defendant, a website designer was pleaded guilty for the hijacking of Arabic language news station ‘Aljazeera’s’ Website during the war in Iraq and he was charged for wire fraud and unlawful interception of an electronic communication in Los Angeles. The AlJazeera’s space channel based in Doha, Qatar was registered in the domain name http://www.Aljazeera.net. The defendant diverted the website and e-mail traffic of the site to MSN Hotmail and changed settings after knowing that this website contained images of American war prisoners and soldiers who were killed during Iraqi operation. He himself informed the FBI about the crime he had committed.

In *United States v. Jeffrey Le Parson*, the defendant was arrested on charge of unauthorized access and attempt to cause significant damage without authorization to the protected computer, Microsoft website etc. violating Title 18, USC Section 1030 (a) (5) (A) (i). The defendant faced a maximum sentence of 10 years in prison, 10 months community service and a $250,000 fine on that charge. He committed the crime by flowing blaster computer worm including ‘W32/Lovesan.worm.b’ which infected more than 7,000 computers of internet users and caused a dangerous damage.

In *United States v. Brett Edward O’Keefe*, the defendant was arrested and charged for conspiracy to gain unauthorized access to government, military and protected computers, also for obtaining financial gain and access to those computers including NASA. The FBI and Army Criminal Investigations Department investigated and ultimately he was arrested.

---

In *United States v. William Sutcliffe*, the defendant was sentenced for making interstate threats to cause injury, killing and posting thousands of social security numbers on websites. He was an employee of Global Crossing as computer technician. After he lost his job he established a website called evilax.com using Global Crossing’s stock symbol and committed this crime.

In *United States v. Robert Lyttle*, the defendant pleaded guilty in Federal Court for hacking into government computers and defacing government websites violating Title 18 USC Section 1030. The defendant was a member of the Deceptive Duo hacking group and admitted that he unlawfully accessed computer system of various government agencies e.g. Department of Defence Logistic Information Service (DLIS), the Office of Health Affairs (OHA) and NASA’s Arms Research Center (ARC) for obtaining files to deface websites hosted on computers. He was ordered to pay about $ 72,000 damages and was sentenced to 3 years supervised release after 4 months in Federal prison.

This is in brief how the USA is fighting against cyber terrorism, be it terrorized use of Information and Technology (ICT) to cause horror, threat to terror people and government; or terrorist groups activities through new technology.

**ix. Prevention and Control of Cyber Terrorism in India**

In 1999, Denning said that ‘Ethnic Tamil Guerillas were said to have swamped Sri Lankan embassies with thousands of e-mail messages. The message was thus “we are the Internet Black Tigers and we are doing this to disrupt your communications, an off-shoot of the Liberation Tiger of Tamil Elam (LTTE).

Nowadays most of the terrorist groups have their own websites or information way (I-way). For e.g., one of the Al-Qaida based websites in Arabic language is [http://www/mojahedoon.net](http://www/mojahedoon.net) which has link with Osama Bin Laden. Information and Communication Technology are very much used by terrorists in India for attack against the nation. Telephone, mobile phone, wireless, computer facilities are available almost everywhere in India. That is why terrorists are able to communicate with each other even being in remote rural area. They can control the entire group activities from remote areas. For e.g Dawood Ibrahim controlling operations of his group from Gulf Country and from

---


Pakistan. In 2000, within 4 months almost 131 Indian websites were defaced and this number was increased in 2001 by 160. The hacker group called “Silver Lords” hacked about 23 Indian websites within 6 days demanding independent Kashmir.325

a. Propensity of terrorists for hacking

In India terrorists are motivated for hacking and defacements of websites. Anti-Indian Crew (AIC), Pakistani Hackers’ Club (PHC), G-Force Pakistan, Pro-Pak Hackers are terrorists groups who are working with Al-Qaida and Bin Laden. Some of these groups are represented by Dr. Neruker who hacked the website of Zee News.

One Anti-India Crew posted in internet was as follows,326 “….Message is for the innocent people being killed in Jammu Kashmir….and U know what’s the reason behind all this killing? Piece of land….I will keep on defacing and passing out this word around the world providing our point….How lame Indians are and their network security is even worse!” On 10th January 2001, Mr. R.K. Ragavan the then Director of CBI said to Info Sec News that a number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them. In July 2005, there were 635 incidents of breaking Indian internet sites.327

Hackers Group called G-Force published the message against India claiming Kashmir. They also had defaced and hacked several websites of Indian Government, companies and scientific organizations. The instance of hijacking of Indian Airlines flight to Kandahar in Afghanistan in December, 1999 is one of such instances of cyber terrorism in India. Terrorists communicated and controlled whole operation through e-mails but it had remained undetected.

In 2001 after Pokhran-II tests western hackers attacked on Bhabha Atomic Research Centre (BARC) to steal nuclear test data.

In May 2001, Indian Government and e-business sectors raised voice to act against anti-Indian hacking especially Pakistani hackers.328 To achieve this goal Government


327 The Times of India, Kolkata, 24th July 2005.

constituted a force on cyber security. According to the Cyber Security Force this is not the attack for attack’s sake rather it is a message to convey that India also can do the same. India is psychologically affected by Pak-hack attacks. Therefore, unlocking the source codes of Pakistani website was taken as a way to prevent and control cyber terrorism in India. In June 2001 the Pakistani Hackers Club defaced Indian website for showing disrespect to the Indian flag. This case was registered on 29th June and the victims as well as the owner of websites which were defaced made a dharna programme in New Delhi as protest against the said attack before the Embassy of Pakistan. Thus India-Pakistan Cyber-War is going on every moment.

According to Dewang Mehta, former President of NASSCOM about 635 Indian websites were hacked during 2000. The awareness on e-security was very poor in India. Companies here were spending only 0.8% of their information technology spending annually as against the world average of 5.5%.

b. Use of telephone and mobile by terrorists

Since 1999 onwards use of mobile phones and e-mail with internet use is increasing day by day among terrorist groups as convenient means to communicate, control and monitor their group. To avoid detections and investigations, the terrorists frequently use different cyber cafes. They are communicating with other terrorist groups worldwide through internet.

c. Attack on the Indian Parliament

On 13th December 2001 attack on the Indian Parliament was with the help of Information Technology. It was a cyber attack, attackers used new technology and committed forgery to fulfill their end. They forged the gate pass and for attack they downloaded the official logo of Ministry of Home Affairs, other documents and the layout of the Parliament building. Police found a laptop from main accused Mohammed Afzal and Shuakat Hussain Guru. Police found out that they accessed the internet through Pakistan based ISPs. Investigating officers also found incoming and outgoing cell phone call numbers of deceased

---

329 Tribune News Service, Ludhiana, Chandigarh, India, 30th June 2001 News publication
330 Ibid.
terrorists which were very much helpful for the police investigation. Police also found out a satellite connection with deceased terrorists cell phone.332

d. Encryption of message

In December 2002, in Kolkata one encrypted message was stored by Mr. S. Kundu’s Cyber Café which contains fears of a terror strike in the city. The owner of the cyber café said that one computer file name was found by his technician. The file name was ‘PAKI_G.BABA0241’ in the D-drive. Out of curiosity he opened the file. It contains misspelling of some famous buildings in Kolkata e.g. Raiters Building, Bikash Bhawan. Farak Bridge, Hoogly Bridge with possible date and time of attack. Thereafter, the Kolkata Police were alerted and due to extra security measures no incident occurred subsequently.333

e. Cyber terrorism in Jammu and Kashmir

In J & K the website and network are used by terrorists for communication between senior commanders in the Kashmir valley and control station. Between Kashmir valley and Doda-Udhampur-Rajauri regions and North-South Pir Panjal range there were Lines of Site (LOS) to provide network facilities. Earlier terrorists used High Frequency Radio Network as means of communication. In May 2003, cellular phones and satellite phone were recovered in Surankat area by army operation. In India, terrorists are also users of BSNL network along with STD and ISD facilities to connect with Pakistan and other countries.334

f. Some new tools used by terrorist

New technology is also producing several new weapons e.g. E-Bomb, High Energy Radio Frequency (HERE) guns, High Altitude Nuclear Explosions, High Power Microwave bombs, Nano-devices, Micro-electromechanical devices coupled with robotics which allow terrorists access to security system and high radiation explosions which cause lose of Low Earth Orbit satellites even within a month. These weapons are used by terrorists worldwide. More than 50 websites provide recipe for making RDX bombs to net users worldwide. Not only that, e-mail system for communication is more reliable way for terrorists. They also have their own websites to express and publish their views.335

Three school boys made a hoax call and disturbed the train scheduled to Sealdah from North Bengal on 26th February night. They made a phone call from their mobile on the way

333 Times of India, New Delhi, on 9th January 2003.
334 Times of India, New Delhi, on 24th May 2003, J&K Shock and Awe Operation
335 Jane’s Defence Weekly, 23rd October 2002
from private tuition to home in evening taking advantage of unlimited free calls offer. As that was last day of the offer they made 22 calls within one hour threatening about blast, loot of house, calls to assistant of MLA representing themselves as extremists from Jharkhand and so forth. Immediately the Calcutta police control room in Lalbazar traced the accused. Due to these terror calls the train was stopped at several destinations and checked, though nothing was found out. Police arrested those boys but said “we grilled the boys for 3 hours. They had committed the nuisance unintentionally. We have cautioned them against doing this in future.  

g. Use of Trojan horse and viruses by terrorists

It was breaking news in India on 16th July, 2005 that a Trojan virus posted as an online CNN news letter containing exclusive video footage of the terrorist attack with the words ‘TERROR HITS LONDON’ and invites recipients to see video shot attachments. The moment recipients started downloading the programme it started copying the users system and access the e-mail servers to send spam and junk mails. The spam mail contains the story of either death of Osama Bin Laden or Saddam Hussein and other data. More than 53,000 computers were affected.  

h. Indian link with Al-Qaida

An Al-Qaida linked group claimed responsibility of suicide bomb and attempted bombing at London. Suspected Al-Qaida linked terrorist and accused of London blast Mohammed Afzal was sentenced to 7 years rigorous imprisonment by Prevention of Terrorist Activities Court on 22nd July 2005. He was charged on conspiracy with his uncle in the UK named Mubarak Musalman Nizam to cause terror and destruction in England, Australia and the USA by hijacking planes, crashing them into vital locations etc. London blasts were the example of cyber terrorism in which we can find Indian link with Al-Qaida. Al-Qaida used internet to effectuate their works easily and quickly.  

In September 2005 Osama Bin Laden threatened India through internet to attack big shopping Mall and places. PTI reported that 15th August 2005 date was declared by terrorists through new information technology that there may be terrorist attack on temples, Airports, Government places.

---

336 “Hoax calls ring alarm”, Alipurduar, West Bengal, 27th February 2008 reported in the Telegraph, Kolkata, 28th February 2008, Bengal, p. 9
337 The Times of India, Kolkata, 16th July 2005.
i. **The Information Technology Act, 2000 and Cyber Terrorism**

The Indian Parliament enacted the IT Act, 2000 with the object to evolve world standard security measures to regulate cyber world and to prevent and control cyber crimes. India cyber crimes are dealt with under our traditional legal system and we do not have special court to deal with the matter. Till now cyber crimes are dealt with following the Cr.PC, the IPC and the IT Act, 2000. NASSCOM President Kiran Karnik also expressed his view towards establishment of Fast Track Court to deal with cyber terrorism.

### I. Protected System

The IT Act, 2000 provides that the appropriate Government may, by notification in the official Gazette, declare any computer resource as protected system because these directly or indirectly affect the facility of critical information infrastructure. The term “critical information infrastructure” means the computer resource which has impact on national security, economy, public health or safety. Any person who is authorized by the appropriate government to access protected systems are called authorized users.

If any person accesses or attempts to secure access to a protected system, it will be treated as contravention of provisions and he shall be punished with imprisonment for a term which may extend to 10 years and shall also be liable to fine. It is the duty of the Central Government to prescribe the information security practices and procedures for such protected system.

### II. Other Preventive and Controlling Measures

If the Central Government is satisfied that it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, security of the State, friendly relation with foreign States or public order or for preventing incitement to the commission of any cognizable offence, then it may by order direct any agency of the Government to intercept, monitor or decrypt information transmitted through any computer resource.

---

339 Section 70
340 Explanation to Section 70 (1)
341 Section 70 (2)
342 Section 70 (3)
343 Section 70 (4)
344 Section 69
For breach of confidentiality and privacy, the IT Act, 2000 prescribes punishment with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.\textsuperscript{345}

If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned disclose such electronic record, book, register, correspondence information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.\textsuperscript{346}

### III. Indian Computer Emergency Response Team

The Indian Computer Emergency Team (CERT – In) shall serve as the national nodal agency in respect of Critical Information Infrastructure for coordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report.\textsuperscript{347} The director of the CERT may call for information pertaining to cyber security from the service providers, intermediaries or any other person.\textsuperscript{348} Failure to supply this information shall be punishable with imprisonment for a term which may extend to 1 year or with find which may extend up to Rs. 1 lakh or with both.\textsuperscript{349}

Cyber terrorism has become one of the complex challenges worldwide in contemporary era of Communication Convergence Technology and globalization as well as liberalization of commerce and business. Terrorists are keener to attack in superhighway because it is not only easier, quicker and cheaper to do so, but also in cyber world it is easy to hide oneself without creating evidence. There is no need of visa to visit other countries because by sitting at homeland they can attack large numbers of targets.

Whoever with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i). denying or cause the denial of access to any person authorized to access computer resource; or

\textsuperscript{345} Section 72
\textsuperscript{346} Section 72
\textsuperscript{347} Section 70 A (1)
\textsuperscript{348} Section 70 A (2)
\textsuperscript{349} Section 70 A (3)
(ii). attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii). introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure commits the offence of cyber terrorism.\(^{350}\)

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access and by means of such conduct obtains access to information, data or computer database that is restricted for reason of the security of the State or foreign relations; or any restricted information, data or computer database with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.\(^{351}\)

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.\(^{352}\)

J. REVIEW

New multimedia technology and internet have become part our daily life in contemporary society and have made life easier, quicker and cheaper. Computers are not only useful for communication and information processing but also useful for typing, editing, drawing, copying, printing, musical purposes, microwave, door keys, remote car driving, to use as remote control, in the form of wireless, mobile phone and so on with ever increasing utility around human society.

Such tremendous utility of Information and Communication Technology (ICT) encouraged the terrorists and other deviants in society to use it sometimes as their tool and sometimes as targets to fulfill their ends.

\(^{350}\) Section 66 F (1) (A)
\(^{351}\) Section 66 F (1) (B)
\(^{352}\) Section 66 F (2).
Cyber terrorism is a kind of cyber threat using new technology. It is national as well as international challenge. Warfare is one way of cyber terrorism by which one nation attacks other nations through information way (I-way). That may be called as net war. International terrorists attack using websites and controlling network i.e., Al-Qaida’a websites http://www.mojahedoon.net which has link with Osama Bin Laden, attack on Indian Parliament on 13th December, 2001 by making false gate pass from internet, 11th September, 2001 attack on WTO and Pentagon controlling network of airway, 16th December, 2005 e-mail threat to attack Indian Parliament and US consulate are examples of cyber terrorism in India.

Internet becomes way to engage in War. That is why cyber war or net war may be called War in the Information Way or I-Way. Taiwan against China, Israel against Palestine, India against Pakistan, China against the USA and so on are some example of Cyber war in I-Way or Superhighway.

For prevention and control of cyber terrorism the national internet security standards must be strong and of world standard.

Especially the Government agencies must choose LAN (Local Area Network) for internal communications and they must adopt their own secret and confidential fiber method about their activities to fight against virus, worm, denial of service attack, attack hacking in net ways which are possible tools and modes of cyber terrorism.

Other most important techniques required to prevent and control attack by terrorists in cyberspace is regular updating of antivirus software, changing passwords and updating of operating system.  

Very important need of the day is awareness, information technology education and training among people who use net and government agencies and even who use non-governmental computer system.

The IT Act, 2000 indirectly prohibits cyber terrorism. But in this regard we need specific and clear law with specific definition of cyber terrorism, legal provisions with specific punishments keeping International and jurisdictional aspects in mind in the era of Global communication convergence and mobile technology.


There is a need for International initiatives to prevent and control net-warfare. Also there is need to improve infrastructure of law enforcing agencies with speedy development of new multimedia technology.

Cyber cafes, ISPs and industries must adopt Bio-metric technologies to prevent cyber crime. It will recognize and record voice, authenticate personal identifications, record fingerprint, finger and hand geometry, record signature verification for e.g. how much time one takes for signature, keystroke, typing and like; record facial features, iris scan i.e. the colored part of eyes and retinal scan, DNA identification, brainwave, ear pattern and like.355

In 2004, the Karnataka State Government passed law requiring cyber cafe patrons to provide proof of identity and other detail information such as name, age, address etc. before use of internet.

There is a great need for establishment of electronic courts and electronic learning process for people in India to prevent and control cyber crimes.356