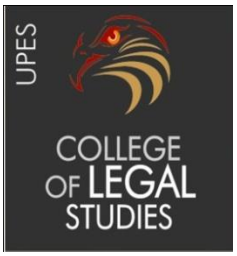
# "CYBER CRIMES UNDER THE INDIAN SCENARIO

**MITALI CHAURE**

**Submitted under the guidance of: Miss. CHARU SHRIVASTAVA**

***This dissertation is submitted in partial fulfillment of the degree of B.B.A. L.L.B(HONS.)***


**College of Legal Studies**

**University of Petroleum and Energy Studies**

**Dehradun**

**2015**

# Acknowledgment

I would sincerely like to convey my deepest gratitude to **Miss. Charu Srivastava Asst. professor ,COLS ,UPES**,who has guided me in the making of this report. She was a source of motivation and encouragement and generated interest in the specific field.

I would also like to thank her for active words of advice and his guidance not only for this report but also for our future and career.

I am also very much alike thankful to **Dr.Tabriz Ahmed Director of COLS, UPES,** who helped & guided me in the making of the dissertation report.

# Declaration

This is to hereby declare that all the work done in this dissertation is genuine and does not infringe any rights relating to copyright act. All the works are referred from some text or report and the footnotings are duly mentioned for the same. All the contents are true and to the best of my knowledge.

# Certificate

This is to certify that **Mitali Chaure** Semester X, B.A.LL.B (Hons.), University of Petroleum and Energy Studies; Dehradun has completed the Second part of his dissertation on **"Cyber Crimes under the Indian Scenario"** under my guidance.

During doing this report he got the exposure of various criminal procedural &substantive laws, international conventions& treaties ensuring the protection of women .She acquired good knowledge of concepts, sense of responsibility, professional judgment and decision making ability.

# Research Methodology

**Doctrinal Research Methodology& *Deductive* Approach** has been adopted in writing this dissertation, Doctrinal research methodology is also known as pure theoretical research. It consists of simple research directed at a specific issue of the law and it's in depth analysis, and in the deductive approach the research is conducted by taking certain generalized notions into account and drawing specific inferences in the light of the fact situations

The Dissertation involves in depth analysis of issues relating to **"Cyber crimes under Indian Scenario** ". The sources used for researching are Books, Internet reports, articles and Court Cases, Statutes etc.

# Index


| Sr. No. | Topics | Page No. |
|---|---|---|
| **1.** | INTRODUCTION TO CYBER CRIMES | |
| **2.** | CLASSIFICATION OF CYBER CRIMES | |
| **3.** | TYPES OF CYBER CRIMES | |
| **4.** | CYBER CRIMINALS | |
| **5.** | COMPUTER RELATED OFFENCES | |
| **6.** | OTHER COMPUTER RELATED OFFENCES | |
| **7.** | CYBER PORNOGRAPHY AND OBESCINETY | |
| **8.** | CHILD PORNOGRAPHY AND OBESCENITY | |
| **9.** | CYBER TERRORISM AND CYBER SECURITY | |
| **10.** | CYBER CRIME AND INFORMATION TECHNOLOGY ACT,2000 | |
| **11.** | CONCLUSION | |
| **12.** | BIBLIOGRAPHY | |

# Abstract

In the current era it is very essential to emphasize here that the world isn't run by weapons any more, or energy or money. It's run by ones and zeros-little bit of data's-it's all electrons. Yes, in today's scenario of online processing, maximum of the information is online which is prone to cyber threats. There are several reasons why computer crime statistics do not reflect the true scope of cyber threats. use the term "dark figure" to refer to undiscovered cyber threats .First, the operational speeds and the storage capacity of computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data processing environment. Third, many victims of computer crimes have failed to crate contingency plants to deal with computer crime. Fourth, once criminal activity has been detected, many businesses have been reluctant to report criminal activity because of fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence,investor loss, or economic repercussions. Therefore, these factors leads a huge number of cyber threats which makes their behavior much difficult to early understanding hence restrict in the early phases of the cyber-attacks. Cyber-attacks having some hidden motivation behind which are processed unknowingly can be considered as the cyber-crime and having serious impacts over the society in the form of economical destruction, psychological disorder, threat to National defense etc. Cyber crime restriction is dependent on proper analysis of their behavior and by studying their impacts over various levels of society. Therefore, the current manuscript will provide the proper understanding of Cyber Frauds and cyber-crimes and their impacts over society with the future trends of cyber-crimes.

# EXCECUTIVE SUMMARY

Cyber crimes are those illegal activities which are committed using computer resources which can be committed either to a computer itself or to a network operations. Cyber crimes are those general kind of illegal activities, which use computers and networks for committing crime. The basic and the for most difference between traditional crimes and cyber crimes is that, the cyber crimes can be multinational or conventional in nature which means it can be operative in several nations or nationalities. Cyber crime is an activity which is committed online in many areas using e-commerce. A computer or any other electronic device like mobile phones etc. can be targeted of committing a crime when unauthorized access of computer , internet networks or online operation occurs and on other hand it also affects E-Business i.e. commerce conducted electronically. Cyber crimes can be classified into different kinds such as Piracy relating to telecommunication, Money Laundering (electronic) and Tax Non payments, Frauds relating to Investment and sales , transferring of Funds through electronic means etc.

The current synchronic epoch has replaced these conventional monetary instruments from a paper and alloy based currency to “elastic money” in the form of credit cards, debit cards, etc. This has a consequence of accelerating the use of debit cards around the world. The utilization of debit cards is not only harmless but is also suited to your comfort. This guard and comfort has unfortunately an evil side as well which does not originate from the use of these debit cards and credit cards rather by the abuse of the same. This wickedness side is implicated in the form of “ATM frauds” that is a worldwide problem. Internet transactions have grown rapidly during the past years and are still growing on and on day by day. But unluckily the apprehension is just not on the expected way because the credit card or the ATM frauds have become the reason for e-business or e-commerce growth. These frauds have become usual on online basis which does not only affects holders of cards but also online traders who are engaged in retail trade. Credit card or ATM frauds can be done by taking over the account, skimming or by stealing etc. Certain preventions could be taken to avoid from becoming a victim of such crimes.

The term "Internet fraud" refers basically to the fraud scheme of any type that utilize one or more elements of the Internet - such as chats between two individuals, e-mail, message boards, or Web sites - to showcase fraudulent appeal to particular victims, to carry out fraudulent transactions, or to convey the proceeds of frauds to financial institutions or to other connected schemes.

# CHAPTER 1: CYBER CRIME

"It is in this digital soup, this is a hyper-relational environment that we see the death of the barrier ... what we do have have is the network and the death of the dichotomy. This is fatal for the legal system, which depends for its very life on the existence of barriers—after all, that's what the law does; it utters the line between this and that, and punishes the transgressor."

—Curtis, A. Karnow

**INTRODUCTION**

As digital technology has advanced over the past 50-odd years, with a force unprecedented in history, governments, businesses and people around the world have been affected immeasurably. The already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary data changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of earlier generations. Perhaps with some of the bias (or naïveté) that is part of our generation, We consider it axiomatic that the changes have included substantial benefits. However, such fundamental restructuring in society also results in certain disadvantages, on all levels.

Our vulnerability increases with the perceived value of and reliance on this technology. Increased opportunities for the industries to be more productive also allow the less-upright new avenues for malevolence. The explosion of new and pertinent statutory law over the past two decades reflects society's attempts to wrestle with an ancient phenomenon in a modern context. Wrongs of all sorts occur all the time, and individuals and organizations address them, if at all, variously in different contexts. But only the sovereign can take a person's life or liberty (as well as property), and then only after due process of law to address the commission of crimes which a legislature has specified in advance. Thus, of all the inequities which significantly involve or revolve around a computer, only those labeled as crimes mark the limits of behavior beyond which certain civil rights of the perpetrator are subject to forfeiture. Coupled with the fascinations of our Information Age, the world of criminal justice provides an interesting vantage point to assess how our complex community tries to restrain itself while racing into the future. It remains to be seen whether the current approaches to deter and redress computer crime will prove successful. Case law has been slow to develop. Most likely, it is still early in a nascent wave of inevitable prosecutions. All elements of law enforcement are themselves—by and large--early in developing an understanding of the nature of these offences and how best to enforce the law.

Let us discuss some of the important concepts/terms associated with the cyber crime.

(i)"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [or any other functions.[1]

(i) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

(ii) "service provider" means:
(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
(b) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

(iv) "traffic data" means any computer data relating to a communication by means of a computer system, generated by the computer system that formed part in the chain of communication, indicating its origin, destination, path or route, time, date, size, duration or type of underlying [network] service.

(iii) "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its service, other than traffic or content data, by which it can be established:
(a) the type of the communication service and equip-ment used by the subscriber and the technical provisions taken thereto, and
(b) the subscriber's identity, address, telephone num-ber, or any other information related to [the subs-criber or] the location of his/her communication equipment.

**DEFINITION OF "COMPUTER CRIME"**

Defined broadly, the term "computer crime" could reasonably include a wide variety of criminal offences, activities, or issues. The potential scope is even larger when using the frequent companion or substitute term "computer-related crime." Given the pervasiveness of computers in everyday life, even in the lives of those who have never operated a computer, there is almost always some non-trivial nexus between crime and computers. This is especially the case when factoring in the extensive use of computers in evidence, investigations, and court administration.

Nevertheless, something far less than such a panoramic view of "computer crime" comes to our mind —when the term is used. And as the phrase is evolving into a term of art, the narrower set of meanings has become more prevalent in the literature. One noteworthy example is the FBI National Computer Crime Squad's (NCCS) list of crime categories it investigates:

[1] Solnick,steven L. "Revolution,Reform and the soviet Telephone System,1917-1927,"Soviet studies,Vol. 43,No.1,1991,157-176.

(i) Intrusions of the Public Switched Network (the tele-phone company);
(ii) Major computer network intrusions;
(iii) Network integrity violations;
(iv) Privacy violations;
(v) Industrial espionage;
(vi) Pirated computer software; and
(vii) Other crimes where the computer is a major factor in committing the criminal offence.

Although its charge limits the NCCS to investigating violations of the Federal Computer Fraud and Abuse Act of 1986.[2], the coverage is still rather broad.

The important point is that Congress defined in that statute all relevant terms necessary to fulfil the constitutional requirements of stating in advance what constitutes criminal behaviour. The same occurs in the legislative creation of all substantive law which outlines criminal offences and their consequences, whether state or federal. Thus, "computer crime" is what the people speaking in their sovereign voice through their elected representatives say it.

The definition of what constitutes a crime on the Internet is still being developed. In the past, the states and federal government have defined cybercrime activities to include the destruction or theft of computer data and programmes to be computer crime. More recently, the definition has expanded to include activities such as forgery, illegal gambling, and cyberstalking.[3]

Both the state and federal governments have laws addressing cybercrime. Cybercrime is being prosecuted under statutes similar to California penal code dealing with unauthorised access to computers, computer systems and computer data[4] or New York's computer law.[5] Both statutes addressed tampering, interfering, damaging or unauthorized access to computer data and computer systems. The Federal government's computer crime statute, 18 U.S.C. sect. 1030 (1995), proscribes the unauthorized use of certain computers and the alteration or destruction of the record they contain.

The development of cyber crime laws has not been without controversy. In 1996, the Federal Government enacted a statute dealing with pornography on the Internet.[6] In the first Internet-related U.S. Supreme Court case Janet Rano vs. American Civil Liberties

[2] (Pub. L. No. 99-474, 100 Stat. 1213 (1986), amending 18 U.S.C. § 1030)
[3] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. *,No.4(1992),PP.243-296.
[4] Latsh:Law in a Digital World:Computer networks and cyber space.38 Vill. L. Rev. 403(1993)
[5] Ronfield,”Cyberocracy”,243-297.
[6] Suri,R.K.,Diwan Parag,Kapoor,S., ”Information technology law”pentagon press,2001

Union,[7] the apex Court held that provisions of the Communication Decency Act,[8] were unconstitutional under the First Amendment.

[7] Ronfield,"Cyberocracy",243-297.

[8] Ronfelter David, "Cybrocracy is coming" The information society journal,Vol. ,No.4(1992),PP.243-296.

## The Scope of Cyber Crime

In 1987 the American Bar Association conducted a survey of three hundred corporations and government agencies regarding the extent of computer crime and their resulting losses. Seventy-two of the respondents claimed to be the victim of computer-related crime within the past twelve months, experiencing losses estimated to range from $145 million to $730 million.[9]

In 1991, a survey of computer related crime of 3,000 Virtual Address Extension sites in the United States, Canada, and Europe was conducted. Eight per cent of the respondents were uncertain whether they had experienced a breach of security. Forty-three per cent of the respondents said they experienced a security incident that had been a criminal offense. Seventy-two per cent of those who responded said they had been the victim of computer-related crime within the past twelve months. [10]

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

There are several reasons by computer crime statistics do not reflect the true scope of computer crime. Criminologists use the term "dark figure" to refer to undiscovered computer crimes. Several factors contribute to this dark figure. First, the operational speeds and storage capacity of computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data processing environment. Third, many victims of computer crime have failed to create contingency plans to deal with computer crime. Fourth, once criminal activity has been detected, many businesses have been reluctant to report criminal activity because of fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions.[11]

[9] Drucker,peter,post-capitalist society(new York,harper business,1993)

[10] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. ,No.4(1992),PP.243-296.

[11] Steward Thomas a.”welcome to revolution”

## Cyber Crime in India

As Republic of India become the fourth highest range of web users within the world, cyber crimes in India has additionally raised 50 % in 2007 over the previous year. In step with the Information Technology (IT) Act, the bulk of offenders were beneath thirty years older. Around 46 % of cyber crimes were associated with incidents of cyber creation, followed by hacking. In step with recent revealed 'Crime in 2007 report', revealed by the National Crime Record Bureau (NCRB), in over 60 % of those cases, offenders were between eighteen and thirty. These cyber-crimes are punishable beneath 2 two categories; the IT Act 2000 and the Indian legal code (IPC). In step with the report, 217 cases of cyber-crime were registered beneath the IT Act in 2007, that is a rise of 50 % from the previous year.[12] Under the IPC section, 339 cases were recorded in 2007 compared to 311 cases in 2006. Out of thirty five mega cities, seventeen cities have according around three hundred cases of cyber-crimes beneath each category that is a rise of 32.6 % during a year.[13] The report additionally shows that cyber crime isn't only limited to railroad cities however it additionally touched to tiny cities like Bhopal. in step with the report, Bhopal, the capital of Madhya Pradesh has according the very best incidence of cyber crimes in the country. [14]In order to tackle with cyber crime, metropolis Police have trained one hundred of its officers in handling cyber crime and placed them in its Economic Offences Wing. These officers were trained for 6 weeks in hardware and computer code, laptop networks comprising data communication networks, network protocols, wireless networks and network security. Teachers at Guru Gobind Singh Indraprastha University (GGSIPU) were the trainers.[15]

[12] Britanica Encyclopedia.com

[13] Paranjape,N.V. " Indian Leagl and Constitutional Hiatory,Central Law agency,allahbad,1994,P.1

[14] Ibid

[15] Cyber crimes-11 del.c.sect 1312 A.

## Cyber Space

As the cases of law-breaking grow; there's a growing have to be compelled to forestall them. Net belongs to everybody. There ought to be surveillance which implies investigators tracking down hackers usually need to watch a cracker as he breaks into a victim's ADPS. The two basic laws governing period surveillance in alternative criminal investigations also apply during this context, search warrants which implies that search warrants could also be obtained to gain access to the premises wherever the cracker is believed to own proof of the crime. Such evidence would come with the pc accustomed commit the crime, yet because the computer code used to gain unauthorized access and alternative proof of the crime. Researchers should explore the issues in bigger detail to find out the origins, methods, and motivations of this growing criminal cluster. Decision-makers in business, government, and law enforcement should react to the current rising body of data.[16] They have to develop policies, methods, and laws to observe incursions, investigate and prosecute the perpetrators, and stop future crimes. additionally, Police Departments ought to at once take steps to protect their own info systems from intrusions (Any entry into a district not antecedently occupied).Internet provides anonymity: this is often one amongst the explanations why criminals attempt to get away easily once caught and additionally offer them an opportunity to commit the crime once more. Therefore, we have a tendency to user should take care. we must always not disclose any personal info on the web or use credit cards and if we discover something suspicious in e-mails or if the system is hacked, it ought to be immediately according to the Police officers United Nations agency investigate cyber-crimes instead of making an attempt to fix the matter by ourselves. Computer crime may be a multi-billion greenback downside.[17] Enforcement should obtain ways in which to keep the drawbacks from overshadowing the good promise of the pc age.[18] Law-breaking is menace that has got to be tackled effectively not solely by the official however additionally by the users by co-operating with the law. The commencement fathers of net wished it to be a boon to the whole world and it's upon US to stay this tool of modernization as a boon and not build it a nemesis to the society.[19]

[16] Gambling—Minn. Stat Sect 609.75(1994)
[17] Britanica Encyclopedia.com
[18] Ronfelter David, "Cybrocracy is coming" The information society journal,Vol. ,No.4(1992),PP.243-296.
[19] Big dummies guide to Internet (online).Available FTP : ftp.eff.org Directory : pub File :bigdummy.txt.

**Computer Crime Categories: How Techno-Criminal Operate**

"It is very essential to emphasize here that the world isn't run by weapons any more, or energy, or money. It's run by ones and zeros—little bits of data—it's all electrons. There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information—what we see and hear, how we work, what we think. It's all about information." Lines from the character "Cosmos," in the movie Sneakers, MCA/Universal Pictures, 1992. The motion picture Sneakers focused on computerized information as a valuable commodity and on the technological means to invade and steal that commodity. To many, the high-tech wizardry of the movie probably appears exotic; however, it is much more realistic than some assume. If there is a lesson to be learned from the movie, it is that the potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes. [20]Discussions of emerging technological crimes' entre mostly on computer crime, with the inference that there is only one type of offence. This is not, however, the case, because specific categories of computer crime exist. As computer-related crimes become more prevalent, an increasing need emerges for police personnel—particularly those who do not have expertise in computer technology—to understand how these crimes vary. An understanding of the types of computer-related crimes will assist law enforcement by providing insight for investigative strategies.[21]

[20] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. ,No.4(1992),PP.243-296.
[21] Drucker,Kaufman, “ Information Technology laws,Pentagone press,2001.

# CHAPTER 2: CLASSIFICATION OF CYBER CRIME

Mr. Pavan Duggal, who is the President of cyber laws, net and consultant, in a report has clearly defined the various categories and types of cybercrimes. Cybercrimes can be basically divided into 3 major categories:

**1.Cyber crimes Against Persons**

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today.[22] The potential harm of such a crime to humanity can hardly be amplified. This is one Cyber crime which threatens to undermine the growth of the younger generation as also leave irreparable cars and injury on the younger generation, if not controlled.

A minor girl in Ahmadabad was lured to a private place through cyber chat by a man, who, along with his friends, attempted to gang-rape her. As some passersby heard her cry, shewas rescued. Another example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe.[23] It is estimated thatthe virus caused 80 million dollars in damages to computers worldwide.

In the United States alone, the virus made its way through 1.2 million computers in one-fifth Of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug".

**2. Cybercrimes Against Property**

The second category of Cybercrimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy.[24]

**3.Cybercrimes Against Government**

The third category of Cybercrimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the

[22] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. ,No.4(1992),PP.243-296.
[23] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. ,No.4(1992),PP.243-296.
[24] Britanica Encyclopedia.com

international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament of India passed its first Cyber law, the Information Technology Act in2000. It not only provides the legal infrastructure for E-commerce in India but also at the sametime, gives draconian powers to the Police to enter and search, without any warrant, any public place for the purpose of nabbing cybercriminals and preventing cybercrime. Also, the Indian Cyber law talks of the arrest of any person who is about to commit a cybercrime.[25] The Act defines five cybercrimes damage to computer source code, hacking, publishing electronic information which is lascivious or prurient, breach of confidentiality and publishing false digital signatures. The Act also specifies that cybercrimes can only be investigated by an official holding no less a rank than that of Dy. Superintendent of Police (Dy.SP).[26]

It is common that many systems operators do not share information when they are victimized by crackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep crackers from gaining access again with as little public attention as possible. According to Sundari Nanda, SP, CBI, "most of the times the victims do not complain, may be because they are aware of the extent of the crime committed against them, or as in the case of business houses, they don't want to confess their system is not secure".[27] As the research shows, computer crime poses a real threat. Those who believe otherwise simply have not been awakened by the massive losses and setbacks experienced by companies worldwide. Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime. Similarly, information systems in government and business alike have been compromised. The economic impact of computer crime is staggering (great difficulty).

[25] Ronfelter David, “Cybrocracy is coming” The information society journal,Vol. ,No.4(1992),PP.243-296.
[26] Times of India “cyber crime” 1997.
[27] Drucker,Kaufman, “ Information Technology laws,Pentagone press,2001.

**ANOTHER SYSTEM OF CLASSIFICATION OF COMPUTER CRIME**

**1. Offences against the confidentiality, integrity and availability of computer data and systems**

**(a) Illegal Access**

The criminal offences by any party when committed intentionally[28] the access to the whole or any part of a computer system without right.[13] A Party may require that the offence be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

**(b) Illegal Interception**

An illegal interception could be defined as criminal offence committed by a party intentionally without right, made by technical means, of non-public[29] transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent.[30]

**(c) Data Interference** A criminal offence when committed intentionally resulting into the damaging, deletion, deterioration, alteration[i] or suppres-sion[17] of computer data without right could be referred as data interference.

**(d) System Interference**

A criminal offence when committed intentionally resulting into the serious hindering without right of the functioning of a computer system by inputting [transmitting] damaging, deleting, deteriorating, altering or suppressing computer data is referred as system interference.

**(e) Illegal Devices**

The criminal offences when committed intentionally and without right:[31]

(a) for the production, sale, procurement, import, distribution or otherwise making

available of:

(i) device, including a computer program, designed or adapted [specifically]

[primarily] [particularly] for the purpose of committing any of the offences mentioned above; and

(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing the offences;

---

[28] Ronald,"cryptograph",pp.39-48

[29] Drucker,Kaufman, " Information Technology laws,Pentagone press,2001.

[30] Stewert Bugeam,the Emerging and Specialised Law of the Digital revolution,los Angeles Dairy journal,jan. 25,1996 at 1.

[31] Britanica Encyclopedia.com

(b) the possession of an item referred to above, with intent that it be used for the purpose of committing the offences. A party may require by law that a number of such items bE possessed before criminal liability attaches.

**2. Computer-related Offences**

**(a) Computer-related Forgery**

The criminal offences when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic,[32] regardless whether or not the data is directly readable and intelligible. A Party may require by law an intent to defraud, or similar dishonest intent, before criminal liability attaches.

"Computer forgery is the alteration of computerized documents." Since, the advent of high-resolution computerized colour laser copiers a new generation of fraudulent counterfeiting has emerged.[33] These copiers can modify existing documents the quality of which is indistinguishable from the original without referring to an expert for analysis. The perpetrators can even create false documents without the necessity of referring to an original document.[34]

**(b) Computer-related Fraud**

Organized crime has used cyberspace to target credit card information, personal and financial information for computer fraud. The sale of this information to counterfeiters of credit cards has proven to be extremely profitable. No longer do bank or credit cards need to be stolen. Counterfeiters using specialized computer hardware and software programs can encode falsified information on credit and bank card magnetic strips.[35] The sale of personal and financial information to create false travel documents had also become big business.[36]

Fraudulent activity has extended to the Internet in the form of fake franchise offerings. In April 1997 the Federal Trade Commission and the North American Securities Administrators' Association, both involved in investigating fraud on the Internet, sent notices to over two hundred web sites which offer business opportunities, warning them that state and federal laws required them to be able to substantiate their earning claims.[37]

---

[32] Ronfelter David, "Cybrocracy is coming" The information society journal,Vol. ,No.4(1992),PP.243-296.

[33] Stewert Bugeam,the Emerging and Specialised Law the Digital revolution,los Angeles Dairy journal,jan. 25,1996

[34] Ronald,"cryptograph",pp.39-48

[35] Drucker,Kaufman, " Information Technology laws,Pentagone press,2001.

[36] *Ibid*

[37] *Ibid*

The criminal offences when committed intentionally and without right, the causing, without right, of a loss of property to another by:

(a) any input, alteration, deletion or suppression of com-puter data,

(b) any interference with the functioning of a computer [program] or system, with the intent of procuring, with-out right, an economic benefit for himself or for another.

**(c) Computer Sabotage**

The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms,[38] viruses[39] or logic bombs[40] is referred to as computer sabotage. Computer sabotage can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists, or to steal data or programs for extortion purposes.[41] In April, 1997 the U.S. Department of Energy Computer Incident Advisory Capability Unit announced that a highly dangerous Trojan horse program capable of deleting all of user's hard disk files was circulating on the Internet. The program was masquerading as AOL4free.com. Its victims were tricked into believing it was a program allowing them to create fraudulent accounts on America Online.[42] In another Internet Trojan horse warning, in August, 1997 AOL warned its online users of a program pretending to be from the AOL Keyword List Area. A user with the screen name KEY List2 sent mail out to some users with an attached file pretending to be the keyword LIST. The purpose of this program was to sniff out user passwords.[43]

**(d) Cyber stalking**

Cyber stalking refers to the activity of users sending harassing or threatening E-mail to other users. Women are especially being targeted by cyber stalkers. For example, a South Carolina woman has been stalked for several years via E-mail by an unknown person who has threatened her life, threatened to rape her daughter, and posted her home address on E-mail making it openly available to anyone with access to the Internet.[44] It has been estimated that approximately 200,000 people stalk someone each year.[45] California was the first state to pass a stalking law. Seven states have passed statutes that include stalking by computer.

3. Content-related Offences

(a) Offences Related to Child Pornography (1) The criminal offences when committed without right and intentionally the following conduct: (a) offering[37] or making

[38] Drucker,Kaufman, " Information Technology laws,Pentagone press,2001.
[39] Paranjpe.N.V.,Op.cit
[40] N-511(U.S.Jun 26,1997)
[41] Janet Reo,op.cit,at 20
[42] Ibid
[43] Rosenor and Smigen,op. cit

[44] Rosenor and Smigen,op. cit
[45] Cager petru, "cyber rising"pp. 66-78

available child pornography through a computer system; (b) distributing or transmitting child pornography through a computer system

# CHAPTER 3 : TYPES OF CYBER CRIME

There are primarily three general types of computer crimes. However, in practice, multiple crimes, that is, concurrent criminality or lesser offences, can occur during any given criminal transaction, resulting in an overlap between the classifications, i.e.,

1. Computer as the target.
2. Computer is incidental to other crime.
3. Crimes associated with the prevalence of computers.

**1. Computer as the Target**

Crimes in which the computer is the target include such offences such as: (i) as theft of intellectual property, (ii) theft of marketing information (e.g., customer lists, pricing data, or marketing plans), or (iii) blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference). These crimes also could entail sabotage of intellectual property, marketing, pricing, or personnel data or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations.)Unlawful access to criminal justice and other government records is another crime that targets the computer directly. This crime covers changing a criminal history; modifying want and warrant information; creating a driver's license, passport, or another document for identification purposes; changing tax records; or gaining access to intelligence files. [46]

Techno-vandalism occurs when unauthorized access to a computer results in damage to files or programs, not so much for profit but for the challenge. In such cases, the damage or loss may be intentional or accidental. Another crime in this category is techno-trespass, that is, "walking" through a computer just to explore. In such cases, the intruder only looks at a file, but even this violates the owner's privacy. This would be the technological equivalent of a criminal trespass. In all of these crimes, the offender uses the computer to obtain information or to damage operating programs. The offender commits the crime either by "superzapping" or by becoming a "super user." These labels mean that the offender accesses the operating program by masquerading as the system's manager, thus giving the intruder access to virtually every file in the system. Not surprisingly, becoming a super user is relatively easy for individuals experienced in computer operations, because virtually every operating system has a trap door that allows individuals to enter a system and declare themselves the system's manager. Trap doors

[46] Barbara Jenson,"cyber Stalking"ACDF journal,pp. 234-247

permit access to systems should a problem, either a human or technological one, arise. Unfortunately, this device also poses a threat to the system's integrity.

One of the best examples of a crime in which the computer is the target can be found in the book, the Cuckoo's Egg by Cliff Stoll. The book recounts the true story of a hacker from Hanover, Germany, who infiltrated a number of computers in the United States, including those of universities, the military, and government contractors. The hacker attempted to locate and steal national security information in order to sell it to foreign governments, a clear illustration of making computers the targets of crime . Computer as the instrumentality of the crime in common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime. In this category, the processes of the computer, not the contents of computer files, facilitate the crime. Essentially, the criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime. Another method involves converting legitimate computer processes for illegitimate purposes. Crimes in this category include fraudulent use of automated teller machine (ATM) cards and accounts; theft of money from accrual, conversion, or transfer accounts; credit card fraud; fraud from computer transactions (stock transfers, sales, or billings); and telecommunications fraud.

One example of using a computer as the instrument to commit a crime is the growing problem of individuals' using cellular phones and electronically billing charges to other customers. In these cases, offenders obtain cellular billing identification codes by using scanning devices, which are small parabolic (curve-shaped) antennae connected to portable computers. When activated, these scanners capture and store account numbers transmitted by cellular phones. The offenders operate near highways, because motorists frequently make calls from their cars. Once they capture the computerized billing codes, they program these codes into other cellular phones simply by hooking up the phone to a personal computer. Then, using software originally developed by programmers in London, they reprogram the signal chip in the cellular phone. The use of this software, which is easy to copy and to use, is spreading across the United States and Canada, sometimes being shared through underground computer bulletin board services (BBS).

**2. Computer is Incidental to other Crimes**

In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act. This means that the crime could occur without the technology; however, computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify and trace. Such crimes include money laundering and unlawful banking transactions, BBSs supporting unlawful activity, organized crime records or books, and book-making. In one

case, a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

Cases involving drug raids, money laundering seizures, and other arrests also have produced computers and electronic storage media containing incriminating information. Many times, the criminals encrypt the data or design the files to erase themselves if not properly accessed. In some instances, criminals even destroy the storage media, such as disks, to eliminate evidence of their illegal activities.

All of these situations require unique data recovery techniques in order to gain access to the evidence. And, in every case, the crimes could occur without the computers; the systems merely facilitate the offences. Another illustration of how criminals use technology to further their illegal activities involves child pornography. Historically, consumers of child pornography have trafficked photographs and related information through newsletters and tightly controlled exchange networks. Now, with the advancement of computer technology, child pornographers exchange this information through BBSs.

Recently, U.S. Customs agents raided 40 locations in 15 States serviced by a Denmark-based, child pornography BBS. These criminals used the computer to facilitate the distribution of pornographic material and to increase the efficiency of criminal activity already occurring via other methods.

3. **Crimes Associated with the Prevalence of Computers**

The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes. In these cases, technological growth essentially creates new crime targets. Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category of computer crime. One offence in this category occurs with relative frequency—the violation of copyright restrictions of commercial software. Initially, this offence may not seem like a serious crime; yet, the potential loss to businesses can be quite staggering. A software package usually costs about $400; a strong-arm robbery usually yields about $50 or less for the thief. Thus, one copyright violation is the economic equivalent of eight strong-arm robberies. However, because the emotional trauma experienced in a piracy is almost non-existent, many people do not view this as a serious crime. Evidence exists that software also is being written and sold explicitly to help hackers break into computers. In another area, successful computer programs—notably word processing, spreadsheets, and databases—are being duplicated, packaged, and sold illegally on a large scale, just as audio and video-tapes are pirated. Similarly, counterfeit computers and peripherals (items such as modems and hard disks)

are being manufactured and sold as originals in much the same manner as imitation Rolex watches and Gucci shoes.[47]

[47] Robert A.guy,Jr. The Nature and the constitutionality of Stalking laws,vo. 4,pp. 12-15

# CHAPTER 4 : CYBER CRIMINALS

Cybercrime is usually committed by a broad range of persons: It may be individual, groups or State viz., students, amateur computer programmers, persons having vested interests, business rivals terrorists and members of organized crime groups. The age of offenders may range from 10 to 60 years and their skill level from novice to professional. There are three basic categories in which we can categorize cyber-criminals: hackers and phreaks, information merchants and mercenaries, and terrorists, extremists and deviants.

**Hackers and phreaks**.—Computers hackers and phreaks (telephone hackers) use information technology to illegally enter computer systems, for the purposes of exploration, information or curiosity. Their crimes, while illegal, are generally not intended to cause damage to data or to reap financial reward. Often hackers and phreaks will engage in pranks, such as re-routing phone calls or rearranging web pages. While their actions may have financial consequences for individuals, corporations or industry, their primary goal is not to profit from their crimes.

**Information merchants and mercenaries.—**In contrast to hackers, information merchants and mercenaries trade in the commercial sale of information, engaging in crimes such as corporate espionage and sabotage, sale and theft of identity information, computer and network break-ins and large-scale software piracy. While they may use similar tools and techniques as hackers, information merchants and mercenaries are primarily driven by profit. Those involved in attaining and selling information often are hired by
competing corporations or are, themselves, former employees for the companies or agencies from which they gather information.

Terrorists, extremists and deviants.—A third group of cyber criminals are those who use cyberspace for illegal political or social activity. In distinction to the first two categories, these cyber-criminals may use internet to engage in terrorism, electronic or otherwise, to promote hate or illegal activities, or to engage in illegal social behaviours such as the transmission of child pornography or engaging in pedophilia online. These groups and individuals often walk the fine line between freedom of expression and illegal activity. This group as cyber criminals is primarily based on internet to engage in illegal activity. This group includes those engaging in information warfare as well as those who use information technology to organize illegal political activity or terrorism.

# CHAPTER 5: COMPUTER RELATED OFFENCES

## 1.Hacking

Hacking means unauthorized access to computers. Those individuals engaged in hacking activities have been termed hackers. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized use or unauthorized access to a computer system. Society is now attempting to come to grips with this new criminal activity, which knows no geographical boundaries and blurs the notion of criminal jurisdiction. Hacking is one of the oldest professions for internet specialists and is definitely the most dangerous cybercrimes. The term hacking is a very wide in nature . A hacker or a supporter of hacking would call it 'quest for knowledge' or `exploring details of a computer and how to stretch their capabilities'. On the other hand, anti-hackers are more inclined to define hacking as 'illegally gaining access to and sometimes tampering with information in a computer'.[48] Hacking may amount to breaking the security system of a website or a computer without the owner's permission or even knowledge, defacing it, denying services to the users of the website, changing the database or even going to the extent of damaging the system by using programmes. It is criminal to use one's own programming abilities, and various programmes with malicious intent to gain unauthorized access to a computer or network. Similarly, the creation and dissemination of harmful computer programmes, which cause irreparable damage to computer systems, are other kinds of cyber crime. Hacking is intrusion of computer system illicitly by users who are not being authorized . The hackers have a wide range of ways to achieve this. The techniques for hacking systems range from stealing password by surfing over the shoulder of someone at work or guessing password or by fooling users into logging in on spoofed sites. None of the computers in the world are completely protected from hacking and every system in the world can be hacked. There is no doubt that hacking is an undesirable phenomenon and criminal hacking is amongst the biggest threats to the internet and e-commerce.

Hacking as a cybercrime is the most dangerous to the internet because it has the effect of eroding the credibility of the internet. Hacking creates a perception in the minds of netizens that the internet is vulnerable and weak.

### Indian Legal provision

Information Technology (Amendment) Act 2008 gives the extended definition of cyber related crimes under amended provision of Section 66: **Section 66 Computer Related Offences' (Substituted vide ITAA 2008).**— This amended provision applies only if the act is done "dishonestly" or fraudulantly". This clause has been re written with significant changes and it applies to all contraventions listed in Section 43 and fine increased to Rs 5 lakhs.

[48] <http://www.waikato.ac.nz/film/studant/0211310B/HannahBower/hrB6-home.html>

Computer related offences as articulated above include every sort of computer related offences. Under this section, if any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable. In other words, to be charged under section 66, any person must cause a computer resource to perform a function with dishonest or fraudulent intent to secure access, knowing that the access he intends to secure is unauthorized. The essential ingredients of this section are:

(a) Unauthorized access to a computer resource; and

(b) Dishonest or fraudulent intent.[49]

It involves an invasion of right and diminution of the value or utility of one's information residing in a computer resource. The accused must have contemplated this when he committed such an offence against a computer resource. Computer related offence involves mental act with destructive animus.

**2.Denial of Service/Distributed Denial of Service Attack**

A Denial-of-Service (DOS) Attack is technique that overwhelms the resources of the target computer resulting in the denial of server access to other computers. In this attack, hackers and crackers prevent or deny access to a computer or web server for legitimate users. In common parlance if a crowd of people surround a department store and block everybody who wants to enter the store, the store in spite of being open cannot provide service to its real customers. This is similar to denial-of-service attacks. The computer criminals through tools send numerous requests to a targeted internet server (usually the web, file transfer protocol, or mail server). This floods the server's resources rendering the system unusable. Any system connected to the internet and running TCP services is vulnerable to such attack. Hackers, to bring down a server, use a number of different techniques and network administrators struggle to control the same but cyber criminals create a more powerful technique. Denial of service is the knocking off. services without permission like through crashing the whole system. Such attacks are easy to launch and difficult to be protected against. There are several reasons for someone crashing a system. They include sub-cultural status, to gain access, revenge, political reasons, economic reasons and nastiness.

The Distributed Denial of Service Attack (DDOS) is a natural development for inflicting more effective and debilitating denial of service attacks. In such attacks instead of using just one computer to launch an attack, the hacker enlists numerous computers to attack the target computer from numerous launch points. In such attacks, a website is bombarded with thousands

[49]In Dr. Vimla vs Delhi Administration, AIR 1963 SC 1572, the Supreme Court has held that " the juxtaposition of the two expressions 'dishonestly' and 'fraudulently' used in the various sections of the Code indicate their close affinity and therefore the definition of one may give colour to the other".

of requests for information in a very short period of time, causing it to grind to a halt. The attack is usually organized from several computers on the web. A hacker secretly plants denial-of-access attack tools on several computers on the web. These computers can be centrally controlled. The methods and resources for executing such flooding differ and are based on the tools used by the hackers.

**3. Viruses**

The construction of viruses, worms logic bombs and Trojan horses, all of which can attack, damage or disarm a computer system or network can be done by anyone having basic knowledge of programming. The growth of these kinds of computer crimes has become far more visible over the past decade. The speed and impact of a virus or worm, which can involve the infection of millions of computers, at work and in the home, probably means that this form of computer crime affects more people than any other forms of cybercrime. The single largest menace facing the world of computers, today, is the threat of corruption and destruction of digital information induced by a human agent with the help of various types of "programmes". The most commonly known programmes can be classified broadly into the following categories:

• Virus[50];
• Worms[51];
• Logic Bombs[52];
• Trojan horse.

Computer viruses are computer programmes like any other programme, except that they cannot run in isolation but require a host to function. People who create them give these programmes an ability to attach themselves to other programmes, to multiply, and damage computer systems, data, or other programmes. Computer virus is designed to replicate and spread, generally without the user's knowledge. When attached to other programmes, they also become a virus carrier. When an infected file is activated or executed or when the computer is started with an infected disk, the virus also gets

[50] A computer virus is a program designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to other programmes (e.g., word processors or spreadsheets application files) or to the boot sector of a disk. When an infected file is activated-or executed-or when the computer is started from an infected disk, the virus itself is also executed. Often, it lurks in computer memory, waiting to infect the next programme that is activated, or the next disk that is accessed at <http: / I www.symantee.com I amenter / reference I corpst.html >

[51] A programme that propagate itself over a network, responding itself as it goes. Nowadays the term has negative connotations, as it is assumed that only crackers write worms. Perhaps, the best-known was Robert T. Morris's `internet Worm' of 1988, a `benign' one that got out of control and hogged hundreds of Suns and VAXen across the U.S. at <http: / / www.netmeg.net /jargon / terms / w / worm.html>

[52] A code surreptitiously inserted into an application or operating system that causes it to perform some . destructive or security-compromising activity whenever specified conditions are met at <http: / / www. huis.hiroshimau.ac.jp / computer /jargon / lexiconentries / logic boms.html>

executed. A properly engineered virus can have an amazing effect on the worldwide internet. For example, the things making big news right now are the Mydoom, MS Blaster worm, the SoBig virus and Sasser. The Melissa virus, which became a global phenomenon in March 1999, was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained. The ILOVEYOU virus in 2000 had a similarly devastating effect. That's pretty impressive when you consider that the Melissa and ILOVEYOU viruses are incredibly simple. Viruses have brought to the forefront the necessity of protecting computers from hackers, crackers, extremists, and computer criminals. Billions of dollars are stolen every year by computer criminals.

**Indian legal provision**

There is no special provision in IT Act for viruses but it is covered under section 43 as explained in hacking.[53] The factors for determining the quantum of compensation are, the amount of gain of unfair advantage, the amount of loss to the victim and the repetitive nature of the default.[54]

*Explanation (i) of Section 43 IT Act defines computer contaminant as, "computer contaminant" means any set of computer instructions that are designed—*

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

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

*Explanation (iii) of Section 43 IT Act defines computer virus as, "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.*

*Explanation (iv) of Section 43 IT Act defines damages as, "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.*

It can be said that the act of planting a virus and other computer contaminants, would also amount to the criminal offence of mischief, which is defined in the Indian Penal Code as follows :[55]

*"Mischief-Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits 'mischief.*

*Explanation 1.—It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is*

[53] "The Menace of Cyber Crime", at <http: / / legalseruiceindia.cont / articles / article+2302682a. ht,n> 2. Sec. 43 (c) of IT Act, 2000

[54] Sec. 47 of IT Act, 2000

[55] Sec. 425 of IPC

*sufficient if he intends to cause, or knows that he is likely to cause, wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.*

*Explanation 2.—Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly."*

**4. Worms**

Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. A worm can wind its way through a network system without the need to be attached to a file, unlike viruses. The computer worm is a computer programme that is designed to rapidly copy itself from one computer to another, leveraging some network medium like e-mail, TCP/IP, etc. They remain hidden in the computer hardware, system software or application software. These worms get activated when certain operations are performed, and cause the intended damage. Worms are basically viruses that do not replicate within other programmes. Instead, they are stand-alone programmes that multiply themselves, stealing system resources such as disk space, input-output cycle and processor cycle. Most viruses rely on some type of user trigger, such as opening an attachment, rebooting a machine, or launching a programme, whereas the worms may be able to operate more independently.

A worm is a parasitic program designed to replicate itself on your worm that appeared on May 3, 2004 were circulating on the internet. New variations of the sasser internet worm are named Sasser.B and Sasser.C. It is similar to an earlier worm, Blaster, because users do not need to receive an e-mail message or open a file to be infected. Instead, just having a vulnerable Windows machine connected to the internet with communications port number 445 is enough to catch Sasser.

**5.Logic Bombs**

A logic bomb may be defined as a programme, which is designed to come into operation at some later date or upon the occurrence of specified conditions. It is a type of Trojan horse used to release a virus, a worm, or some other destructive code. Logic bombs are triggered at a certain point in time or by an event or an action performed by a user. An action can be pressing of certain keystrokes or running a specific program. An event may be loading a backup tape or the birthday of a famous person.

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate it, merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. In several cases a programmer told the logic bomb to destroy data if the company payroll is run and

his name is not on it. The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn't find the employee's name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well.

**6.Trojan Horse**

A Trojan horse is a method for inserting instructions in a program so that program performs an unauthorized function while apparently performing a useful one. Trojan horses are a commonly used method for committing computer-based fraud and are very hard to detect. A Trojan (or Trojan horse) is a malicious program that pretends to be a benign application. It is designed to cause your computer to do something that is unexpected. Since it does not spread (not self-replicating) it is not really a virus. A Trojan horse program contains codes intended to disrupt a computer system or e-commerce site.

# CHAPTER 6 : OTHER COMPUTER RELATED OFFENCES

### 1. Cyberstalking/Cyber harassment

As she stares at her computer, she thinks whether to go online today? Lately she has been bombarded with hate mail, e-mail bombs, on-line verbal abuse and electronic viruses. Even her telephone has been ringing continuously with people on the other line saying weird things and that the pictures of her on the internet were great. She feels scared and threatened. This can be termed as a case of cyberstalking or harassment. Nearly four years ago, the word cyberstalking was not yet coined. No one knew what to call it; some called it online harassment, online abuse, or cyber harassment. There were incidents where it had gone beyond an annoyance and had become frightening. As more and more incidents became known and victims reached out to law enforcement agencies for help, there was no remedy or were told to turn off their computer. There were no laws in place to protect such victims, and their harassers went unabated, which escalated sometimes to real-life stalking situations. Stalking is a legal term that has different definition in different states. What these legal terms generally boil down to is that stalking is a deliberate course of action that causes another person to be afraid. In very general terms, stalking refers to harassing or threatening behaviour that an individual engages in repeatedly towards another person.' In quasi-legal terms, stalking can be defined as a 'willful course of conduct' that 'actually causes' the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested and that would cause a 'reasonable person' to feel so. These actions can include (but are not limited to) following, verbal threats, repeated phone calls, hang up calls, spying, harassment, bothering the friends, family, and/or co-workers of the victim, letters and notes, e-mail, hiding outside your house, etc. Though stalking is not a violent crime, yet it may escalate to serious forms of crime. But again these are separate crimes with separate charges.

Stalking does not amount to breaking and entering, battery, assault, pedophilia, child pornography, or any other such like crime. Stalking is a vivid example of how the internet can provide new opportunities for committing crimes and can create completely new forms of crime. Victims can be stalked on the internet through a variety of means. Receiving unsolicited e-mails containing obscene or threatening messages, having invasive, defamatory or even pornographic images posted on the web or distributed widely through e-mails or even taking over a victims' computer are all means used to stalk in cyberspace.

### 2.Cyber harassment

Black's Law Dictionary defines harassment as, "A course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose" or "words, gestures, and actions which tend to annoy, alarm and abuse (verbally) another person." Electronic Harassment in the workplace is a new category of threatening behaviour. The

offenders misuse corporate resources to harass co-workers, invade and even track their privacy whereabouts. The company becomes liable, not only due to the harasser's status of employee, but because they actually make their company a party to the harassment by using company resources to harass co-workers. The onus is on the company to take effective and appropriate action to terminate the harassment.

**Harassment occurrences**

There are generally two types of harassment on the net-through electronic mail and during chats on an IRC. These messages take many forms: inappropriate sexually explicit language; unwelcome questions about one's physical appearance or sexual practices; or threatening or hostile messages.

Cyber harassment can occur in many forms and some examples are as under :

• Abusive communications via chat or email, or obscene or disgusting pictures;

• Threat of death or bodily harm;

• Following around like a lovesick puppy and pestered over a prolonged period of time by someone who tells that they are in love;

• A series of electronic attacks on internet connection, disconnecting over and over again;

• Get electronic viruses to try to cause.problems on the computer;

• Nasty, cruel or defamatory things written about the victim on someone's web site or in a post they make to a discussion group;

• Unsolicited email;

• Live Chat;

• Hostile Usenet Postings about you;

• Spreading vicious rumors about you;

• Leaving abusive messages on site guest books;

• Impersonation thr victim online;

• Electronic sabotage, (sending viruses, etc);

• Threatening phone calls;

• Threatening mail.

**Indian legislative provisions**

India is at the threshold of tremendous growth in the internet industry. As the penetration of internet is growing, new and complex issues concerning cyberlaw are emerging. Cybercrime is one particular area where one sees a great deal of activity. Cyberstalking is one of the latest crimes that have emerged in India.

Ritu Kohli's case is India's first case of cyber stalking, which was registered by Economic Offences Wing of Delhi Police under Section 509 IPC for outraging the modesty of a woman. As reported, a disgruntled colleague of the husband of Mrs. Ritu Kohli started chatting on the internet through the website www.mirc.com, under the identity of Ritu Kohli, using obscene language. He was distributing Ritu Kohli's residence telephone number to net users and inviting them to chat with her on telephone. The matter came to light when Ritu Kohli started receiving obscene phone calls from different quarters from India and abroad. On inquiry from the callers, it was found that the telephone number was obtained from the net. The matter was then reported to the police. The police asked Ritu Kohli to log on to the website as a male and chat with the person, who called himself Ritu Kohli. The police was therefore able to trace the relevant IP address, the telephone number of the offender and catch him. Delhi Police arrested Manish Kathuria in India's first case of cyberstalking.

This is the first time when a case of cyberstalking has been reported. Cyberstalking does not have any one definition but it can be defined to mean threatening, unwarranted behaviour or advances directed by one net user to another user using the medium of internet and other forms of online.

The case of Ritu Kohli raises the crucial question as to what exactly is Cyberstalking? Cyberstalking is defined as unwarranted, threatening behavioral patterns or advances directed by one internet user against another with the purpose of harassing the other user, by using the medium of internet. Cyberstalking is a relatively new phenomenon.

Unfortunately, the IT Act, 2000 contains no provisions addressing this issue. Until the government takes action to protect users, users must take action to protect themselves by appling sec. 503-507 of IPC.

**But now after the Information Technology (Amendment) Act 2008**

Cyber stalking is one of the recognized cyber crime in India under Section 66 A.

**Section 66-A Punishment for sending offensive messages through communication service, etc. ( Introduced vide ITAA 2008)**

The above mentioned section creates an onus on the sender of the message, not to send any message by means of a computer resource[56] or a communication device[57], which may be:

(a) Grossly offensive or menacing in character; or

(b) Known to be false, but is being sent purposefully and persistently to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatered, or ill will; or

(c) Cause annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.[58]

Such messages can be in the form of text (e-mails, SMSes, blogs, vblogs, tweets[59]), image, sound, voice (VoIP[60]) etc. However, it is to be seen from the recipient's perspective about the nature of harm caused to him by the sender's messages(s).[61]

**2. E-Mail bombings**

Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing. Sending numerous or large e-mail message to one person is considered "e-mail bombing." Software can be written that will instruct a computer to do almost anything, and terrorism has hit the internet in the form of mail bombings. By instructing a computer to repeatedly send electronic mail (e-mail) to a specified person's e-mail addressCyberlaw.[62] But with the Information Technology (Amendment) Act 2008 some provisions of Section 66A, 66B, 66C, 66D deal with web related crimes.

**3.Cyber Fraud, Identity theft and Cyber Cheating**

Cyber fraud often makes headline news but it is thought that the number of cases of fraud detected and prosecuted is just the tip of the iceberg.[63] Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the internet itself.[64] All the

[56] Section 2(1)(k)
[57] Section 2 (1)(ha)
[58] Stripping of headers and footers details from emails to avoid detection; spoofing IP address etc.
[59] Tweets are short messages, which are being used on micro-blogging site, tweitter.com
[60] Voice over Internet Telephone services, like gTalk, skype etc.
[61]Vakul Sharma, "Information Technology Law and Practice Law &Emerging Technology Cyber Law & E-commerce", 3rd Edition, p 182
[62] "Hackers getting even more ingenious" at <http: 11 www.economictimes.indiatimes.com 1 articles how 1 msid-415933- prtpage- 1. cms>
[63] David Bainbridge, "Introduction to Computer Law", at 291 (2000)
[64] For our purposes, the term "internet fraud" may be broadly defined as any fraud committed through or with the aid of computer programming or internet-related communications such as web sites, email, and chat rooms.

major financial institutions throughout the world, use computers to carry out their business and vast sums of money are transferred through computers (electronic funds transfer). Fraud on the internet constitutes about one-third of all cyber crimes.' Internet fraud and forgery have increased substantially by 29% over the past year.[65] It is the most profitable business on the internet. Cyber frauds are waiting for e-commerce to unleash its full potential becausetheir profitability is directly linked with the growth of e-commerce. In fact, most cyber frauds are not disclosed by the victims because of the fear of loss of public trust, confidence, image and business. Some of the major areas of fraud and cheating on the internet include misuse of credit cards by obtaining passwords by hacking, bogus investment/get rich schemes, deceptive investment newsletters containing false information about companies, non-delivery of goods purchased from online auctions and websites, misappropriation and transfer of funds, etc.'[66]Online fraud, today, poses a major threat to the continued popularity of e-commerce[67]. For our purposes, the term "internet fraud" may be broadly defined as any fraud committed through or with the aid of computer programming or internet-related communications such as websites, email, and chat rooms[68]. Misrepresentation may also be innocently made. If a person makes a statement that he or she believes to be true but that actually misrepresents material facts, innocent misrepresentation, not fraud, has occurred. In this situation, the aggrieved party can rescind (cancel) the contract but usually cannot seek damages.

**Indian legal persepective**

Section 66C and section 66D deals with the cyber fraud, data theft, identity theft, phishing, cheating, clone, email fraud, email forgery, etc.

**Section 66C Punishment for identity theft (Inserted Vide ITA 2008)**

This section is meant to protect the identity of a user in the online medium. The objective of the section is to protect the privacy of all or any online users, including their personal information or data. The perspective of the aforesaid section is not to merely protect the information residing in a computer resource but to protect the authentication details of any person in the form of electronic signatures (including digital signatures), passwords, PINs, biometric identifiers or any such other unique identification feature. This section treats "identity" of a person as his authenticating feature, and whoever, intending to take such an "identity" dishonestly or fraudulently, out of the possession of any such person is committing an offence. This section is about the loss of movable property, which may be in the form of electronic signature, password or any other unique identification feature of any such affected person. Further, it protects integrity and security of computer resources from attacks by unauthorized persons seeking to enter such resources, whatever may be their intention or motive. The offence of identity theft is

[65] "WebCrimeStatistics"at <http 1 /www.intergov.org>

[66] Vivek Sood, "Cyber Law simplified", at 50 (2001)

[67] Michael Adler, "Cyberspace General Searches and Digital Contraband", 105 (4) Yale Law Journal 1093 (1996)

[68] Financial Times, 24 Apr 97

completed when there is a dishonest or fraudulent downloading, copying or extraction of the electronic signature, password or any other unique identification feature of any other person. In other words, the moment personal information is downloaded, copied or extracted of any person — dishonestly or fraudently, mens rea comes into existence. Whether the offendor makes use of such downloaded, copied or extracted personal information will be the actus reus component of the crime. This section is meant to protect all e-commerce and e-governance services users.[69]

**Section 66D Punishments for cheating by personation by using computer resource (Inserted Vide ITA 2008)**

The key ingredient of this section is "cheating by personation by means of any communication device' or computer resource[70]. Cheating by personation by using computer resources require: (1) Whoever,

(2) by deception of any person,

(3) (a) fraudulently or dishonestly including that person by personation—

(i) to accept, agree, transact or deliver any data, information to any person; or

(ii) to consent that any person shall retain any data, information etc; or

(b) intentionally inducing that person to do or omit to do anything which he would not do or omit, if he were not so deceived by such personation;

**5. Phishing**

Phishing is also known as "brand spoofing" or "carding"[71] is a process employing the immense capabilities of the internet to socially engineer people by imitating legitimate forms and methods into imparting their confidential information for purposes of identity theft. "Phishing is a particularly incidious attack on the internet community because it almost always involves two separate acts of fraud. The phisher first 'steals' the identity of the business it is impersonating and then acquires the personal information of the unwitting customers who fall for the impersonation. This has ledcommentators to refer to phishing as a 'twofold scam' and a `cybercrime double play."[72]

---

[69] Vakul Sharma, "Information Technology Law and Practice Law &Emerging Technology Cyber Law & E-commerce", 3rd Edition, p 185-186

[70]

[71] The term "social engineering" has been popularized in recent years by reformed computer criminal and security consultant Kevin Mitnick who points out that it is much easier to trick someone into giving their password for a system than to spend the effort to hack in. See.
<http://en.wikipedia.org/wiki/Social_engineering_%28security%29# cite_note-CSEPS-4-7>

[72] Robert Louis B. Stevenson, "Plugging the Thishing' Hole: Legislation Versus Technology 2005", Duke L & Tech Rev 6(2005).

**The Delhi High Court opined in National Assn. of Software and Service Companies v. Ajay Sood[73] that,**

Phishing is a form of internet fraud. In a case of `phishing, a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords, etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party. Typically `phishing' scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

In United States v. Kalin, [74] the defendant registered four websites with domain names deceptively similar to the website operated by DealerTrack Inc. DealerTrack provides services via internet to auto dealerships located throughout US, including dealers' ordering credit reports on prospective automobile buyers. The defendant's website was designed to be practically identical to the main page of DealerTrack. He then got a number of dealership employees mistakenly enter usernames and passwords at his sites and consequently managed to obtain unauthorised access to DealerTrack for personal data.

**Indian Legal Provision**

In India, the Information Technology Act, 2000 and its subsequent 2008 Amendment cover the phishing scenario. The phishing fraud is an online fraud in which the fraudster disguise themselves and use false and fraudulent websites of bank and other financial institutions, URL Links to deceive people into disclosing valuable personal data, later on which is used to swindle money from victim account. Thus, essentially it is a cyber crime and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding some new provisions to deal with the phishing activity. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:

Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently. effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act.

Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000.

Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.

[73] (2005) 119 DLT 596 at pp. 598-99 : (2005) 30 PTC 437 (Del).
[74] 2. DNJ, Nov. 2003.

Section 66D: The fraudsters through the use of the phishing email ontaining the link to the fake website of the bank or organizations ersonates the Bank or financial institutions to cheat upon the innocent ersons, thus the offence under Section 66D too is attracted.

# CHAPTER 7: CYBER PORNOGRAPHY ANY CYBER OBESCINETY

**Definition**

Pornography has been defined in the Oxford Dictionary as The explicit description or exhibition of sexual subjects or activity in literature, painting, films, etc., in a manner intended to stimulate erotic rather than aesthetic feelings; literature etc. containing this. The Webster Dictionary defines pornography as `(i) writings, pictures, etc. intended primarily to arouse sexual desire; (ii) the production of such writings, pictures, etc'. Technically, `pornography' has come to the English language from the Greek language Tornographos' (riorne prostitute + graphein write).' Hence, it begins with `porne or porno' which means 'prostitution', which further implies that the subject is not mutual love, or love at all, but domination and violence against women. It ends with a root `graphos', which means 'writing about' or `description of which puts still more distance between the subject and object. Thus it induces a spontaneous deep desire for closeness with object and voyeur, a dangerous situation rendering a person to become a covert, passive and powerless observer of the pornographic activities written or otherwise available in cyberspace.

R.D. Udeshi v. State. of Maharashtra' is an important case, which defines 'obscenity' in the Indian context. Obscenity is defined as things that deprave or corrupt those whose minds are open to such immoral influences. It also stated that intention was not needed.'

"Obscenity," however, is a legal term, which was defined by the U.S. Supreme Court in its 1973 Miller v. California' decision. For something to be found obscene, and therefore unprotected by the First Amendment, a judge or jury representing a cross section of the community must determine if the material:

- Taken as a whold, appeals to a prurient (sick, morbid, shameful, or lascivious) interest in sex;
- Depicts sexual conduct in a patently offensive manner (i.e., goes beyond contemporary community standards with regards to depictions of sexual conduct or activity); and
- Taken as a whole, lacks serious literary, artistic, political, and scientific value.

**Indian legal Provision**

The term "sexually explicit act or conduct" has been qualified by the word "explicit", meaning thereby that mere obscene act or conduct' may not fall under this section. For punishment under this section — "publication or transmission of sexually explicit act or conduct" — is an essential ingredient.

the difference between section 67 and 67A depends on the nature of cene content.

| | Section 67 | Section 67 A |
|---|---|---|
| Nature of offence | Punishment for publishing or transmitting | Punishment for publishing or transmitting sexually explicit act or conduct |
| Applicability | Generic | Specific |
| Test of obscenity | Likely audience test to prove obscenity | Nolikely-audience test Whether content in question- is it patently or grossly |
| Punishment | First conviction-three years, and fine which | First conviction- Five years, and fine which may extend to ten lakh rupees |

# CHAPTER 8 : CHILD PORNOGRAPHY AND OBESCINETY

## Child Pornography

Child pornography refers to images or films (also known as child abuse images) and in some cases writings depicting sexually explicit activities involving a child; as such, child pornography is a record of Child Sexual Abuse. Abuse of the child occurs during the sexual acts which are recorded in the production of child pornography and several professors of psychology state that memories of the abuse are maintained as long as visual records exist, are accessed, and are "exploited perversely."

To define child pornography is not an easy task. According to UNCRC the child pornography includes any representation of a child engaged in real or stimulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes. European Union defines as "any audio visual material, which uses children in sexual context". International Criminal Police organization (Interpol) defines child Pornography as "means of depicting or promoting sexual, abuse of a child, including print and/ or audio, centered on sex acts or genital organs of children". United States defines as "permanent record of sexual exploitation or abuse of an actual child.'

In United State of America, the Child pornography prevention Act 1996 defined child pornography as, "any depictions, including any photography, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where:

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

(b) Such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct

(c) Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or

(d) 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".[75]

[75] ICFAI at 159

**Indian legal provision**

**67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form—**

Explanation.—For the purposes of this section, "children" means a person who has not completed the age of 18 years.

In view of India's international commitment, especially being signatory to Convention on the Rights of the Child and ratifying the 'Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography' — the introduction of the aforesaid section in the Information Technology Act was long awaited.

The aforesaid section criminalizes all kinds of online child pornography. The term online refers to publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. As provided in the Explanation clause, "children" means a person who has not completed the age of 18 years. Under the said section, five instances of online child pornography has been criminalized:

(a) publishing or transmitting or causing to publish or transmit material in any electronic form which depicts children engaged in sexually explicit act or conduct;

(b) creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing material in any electronic form depicting children in obscene or indecent or sexually explicit manner;

(c) cultivating, enticing or inducing children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource;

(d) facilitating abusing children online, and

(e) recording in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

Although under section 67B, five instances of online child pornography has been criminalized, but it is obligatory to note that clauses (a) and (e) are generic in nature, whereas clauses (b), (c) and (d) are specific.

# CHAPTER 9 : CYBER TERRORISM AND CYBER SECURITY

**Definition**

The combination of two of the greatest fears of the late twentieth century lay in the term "cyber terrorism". Terrorism is the calculated and unlawful use of force or violence, or threat of force or violence, against persons or property to inculcate fear, intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of goals that are generally religious, political, or ideological. Cyberspace is the "virtual world". Barry Collin defines the virtual world as "symbolic - true, false, binary, metaphoric representations of information - that place in which computer programs function and data moves."' Therefore, Cyber Terrorism is the definition of Terrorism with the addition, "through the exploitation of computerized systems deployed by the target

The FBI definition of terrorism.—"The unlawful use of force or violence against persons or property to intimidate or coerce a government, the .civilian population, or any segment thereof, in furtherance of political or social objectives."

U.S. Department of State definition of terrorism.—"Premeditated politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents"

Definition of Cyber Terrorism.—The FBI defined cyber terrorism as "The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents".

The U.S. National Infrastructure Protection Center defined the term as.—"A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda".

**Indian legal Provision**

**Section 66F Punishment for Cyber Crime**

This section is a combination of sections 66, 70 of the Act[76]. What separates section 66F from other sections is degree and nature of offence. If using a sliding scale approach to measure the gravity of offence, section 66 is at one end of the spectrum, whereas section 66F is at the other end of the spectrum.

| Penalty | Section 66 | Section 70 | Section 66F |
|---|---|---|---|
| Imprisonment term | May extend to three years | may extend to ten years | May exten to imprisonment for life |

Cyber terrorism as an offence exists in three forms. Essential ingredients of these three forms of cyber terrorism are:

**Form I:**

1. An intention to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, by

(a) Denying or causing the denial of access to any person authorized to access computer resource; or

(b) Attempting or causing to introduce any computer resource without authorisation or exceeding authorized access; or

(c) Introducing or causing to introduce any computer contamiant. thereby,

2. Causing or likely to cause (i) death or injuries to persons' , or (ii)

damage or destruction of property, or (iii) damage or disruption of supplies or

[76] Sections 69 and 69A are preventive sections and hence not include.

Services essential to the life of the community, or (iv) disruption of or affection the critical information infrastructure, as specified in section 70.

OR

**Form II:**

1. Knowingly or intentionally penetrating or accessing a computer resource without authorization or exceeding authorized access, and

2. Thereby information, data or computer database, which is restricted for reasons of the security of the State or foreign relations.

OR

**Form III:**

1. Knowingly or intentionally penetrating or accessing a computer resource without authorization or exceeding authorized access, and

2. Thereby obtaining access to restricted information, data or computer database,

3. With reasons to believe that such restricted information, data or computer database may cause or likely to cause injury to: (i) the interests of sovereignty and integrity of India, the security of the State, the security of the State friendly relations with foreign States, pubic order, decency or morality, or (ii) in relation to contempt of court, (iii) defamation, or (iv) incitement to an offence, or (v) the advantage of any foreign nation, group of individuals or otherwise.

## CHAPTER10:CYBER CRIME AND INFORMATION TECHNOLOGY AMENDMENT ACT,2008

### Information Technology Amendment Act, 2008

The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions; data security, data privacy and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they required harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, thus it hadbecome necessary to declare such infrastructure as protected system, so as to restrict unauthorised access. Further, a rapid increase in the use of computer and Internet has given rise to new forms of crimes like, sending offensive emails and multimedia messages, child pornography, cyber terrorism, publishing sexually explicit materials in electronic form, video voyeurism, breach of confidentiality and leakage of data by intermediary, e-commerce frauds like cheating by personation - commonly known as phishing, identity theft, frauds on online auction sites, etc. So, penal provisions were required to be included in the Information Technology Act, 2000. Also, the Act needed to be technology-neutral to provide for alternative technology of electronic signature for bringing harmonization with Model Law on Electronic Signatures adopted by United Nations Commission on International Trade Law (UNCITRAL)

Keeping in view the above, Government had introduced the Information Technology (Amendment) Bill, 2006 in the Lok Sabha on 15th December 2006. Both Houses of Parliament passed the Bill on 23rd December 2008. Subsequently the Information Technology (Amendment) Act, 2008 received the assent of President on 5th February 2009 and was notified in the Gazette of India.

**IT Act Amendment which came into force after Presidential assent in Feb 2009 has following salient features**:

Liability of body corporate towards Sensitive Personal Data New amendment was brought in changes in section 43 of IT Act 2000 in which for the first time any body corporate which deals with sensitive personal information does not have adequate controls resulting in Wrongful loss or wrongful gain to any person is liable to pay damages to that person to the tune of five crores.

**Introduction of virus, manipulating accounts, denial of services etc made punishable Section 66 has been amended to include offences punishable**

as per section 43 which has also been amended to include offences as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both. This is a change from earlier position where introduction of virus, manipulating some ones account has been made punishable with imprisonment for the first time.

**Phishing and Spam**

While this has not been mentioned specifically but this can be interpreted in the provisions mentioned here in section 66 A. Through this section sending of menacing, annoying messages and also misleading information about the origin of the message has become punishable with imprisonment up to three years and fine.

**Stolen Computer resource or communication device**

Newly added Section 66B has been introduced to tackle with acts of dishonestly receiving and retaining any stolen computer resource. This has also been made punishable with three years or fine of one lakh rupees or both.

**Misuse of Digital Signature**

Section 66C. Dishonest use of somebody else's digital signature has been made punishable with imprisonment which may extend to three years and shall also be liable to fine with may extend to rupees one lakh. Cheating Cheating using computer resource has been made punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee (section 66D)

**Cyber terrorism**

The newly introduced section 66F talks about acts of cyber terror which threatens the unity, integrity or sovereignty of India or strike terror in the people or any section of the people include

a. Denial of service of resources in use by nation

b. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access

c. Introducing or causing to introduce any computer contaminant likely to cause death or injuries to person or damage to or destruction of property or disrupts knowingly that it is likely to cause damage or disruption of supplies or services essential to the life of the community or

d. knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data

or computer database that is restriced for reasons for the security of the State or foreign relations, or any restrictued information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or is 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. These acts have been made punishable with Imprisonment which may extend to imprisonment for life

**Child Pornography**

Newly introduced section 67 B attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, any one who creates, facilitates or records these acts and images punishable with imprisonment of five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence.

**Intermediary's liability**

Intermediaries have been made liable to retain any information in the format that Central government prescribes. (Sections 67C) and are punishable for violation with a punishment of imprisonment of 3 years and fine. In case of any act which affects national sovereignty intermediaries are liable to seven years (Section 69(4))

**Surveillance, Interception and Monitoring**

In order to compact cyber terrorism the government has further armed itself with drastic powers Sections 69 of IT Act 2000 amended enhances the scope from the 2000 version to include interception and monitoring. This has been a major change in the section which also empowers government not only to monitor any traffic but also block any site through any intermediary. Any failure on part of the intermediary is punishable by seven years and also fine (Section 69(4)). Earlier the provision did not mention any fine.

**Cognizance of cases**

All cases which entail punishment of three years or more have been made cognizable. Offences with three years punishment have also been made bailable (Section 77B). This change though welcome will make sure most cases falling under IT Act will be bailable with sole exception of Cyber terrorism cases, cases related to child pornography and violations by intermediaries in some cases.

**Investigation of Offences**

One major change has been inclusion of Inspectors as investigating officers for offences defined in this act (section 78). Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because number of officers in this rank is limited. With this change one can look forward to more cases being filed and investigated by police.

**Major Dilutions**

**Sexually explicit content:** Newly introduced section 66 E talks about acts of 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 three years or with fine not exceeding two lakh rupees, or with both. In fact the earlier section 67 of IT Act did mention 'any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave..' and was punishable for first offence with five years of imprisonment and fine of one lakh rupees. This change has made the provision lenient and open to misinterpretation.

**Compliance with orders of Controller**

Section 68(2) which earlier made failure to comply with the direction of controller punishable with three years of imprisonment or fine of two lacks or both now has been reduced to two years punishment or fine of one lakh of rupees or both. Indian IT act Amendment though has made a major attempt to address issues related to cyber crime, it still falls short on many counts. Some of the major shortcoming which we feel need to be addressed are:

**Pornography**

Section 67 of the IT Act lays down the law that obscenity is an offence when it is published or transmitted or caused to be published in any electronic form. The expressions, 'publishing' or 'transmission' have not been specifically defined under the IT Act.

**Data Protection**

The Information Technology Act talks about unauthorized access in section 43 of the IT Act but it does not talk about maintaining integrity of customer transactions. U.K has a data protection law which was enacted 10 years back that is in 1998[77]under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data.

**Spamming**

Spamming is a growing menace and India figures in top 10 countries as originators of spam. Still this has not been addressed in the manner it should consider the wastage it causes. One may

[77] Data protection Act 1998,UK: http://www.opsi.gov.uk/Acts/Acts 1998/ukpga_en_1

argue that section 43 of IT Act[78] while referring to "(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;" deals with spam. This however leaves a lot to interpretation.

**Identity Theft**

Identity theft worldwide is a growing problem. IT act 2000 fails to address this issue. This is a major drawback considering the fact that majority of outsourcing work that India does, requires the companies in India to ensure there is no identity theft. In fact identity theft was one of the main reasons for a major hue and cry over an incident involving personal information of UK customers and an Indian web marketing company.[79] As country develops into a more robust economy and use of computers becomes ubiquitous, it is imperatNe that our laws are updated to respond to changing scenario. Quite unlike other penal laws IT Act in particular needs revision and reviews much more regularly mainly due to rapid changes in use of Information Technology.

The IT Amendment Act 2008 brings about various sweeping changes in the existing Cyberlaw. While the lawmakers have to be complemented for their appreciable work removing various deficiencies in the Indian Cyberlaw and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; a legislation that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world.

According to Information Technology Act, 2000 Chapter XI deals with offences or computer crimes and provides for penalties for these offences. The nature of criminal offences and punishments are given below:

| SECTION | NATURE OF | PUNISHMENT |
|---|---|---|

[78] IT Act : http://www.legalserviceindia.com/cyber/itact.html
[79] Horror of outsourcing to India.http://www.indiadaily.com/editorial/4198.asp

| | OFFENCE | |
|---|---|---|
| Section 65 | Tampering with computer system source code documents | Imprisonment upto 3 years or with a fine upto Rs. 2 lakh or with both. |
| Section 66(2) | Hacking with computer systems | Imprisonment upto 3 years or with a fine upto Rs. 2 lakh or with both. |
| Section 67 | Publishing or transmitting obscene material is electronic form | Imprisonment upto 5 years or with a fine upto Rs. 1 lakh for first conviction.<br>Imprisonment upto 10 years or with a fine upto Rs. 2 lakh for subsequent conviction. |
| Section 71 | Misrepresentation or suppression of material facts to controller or Certifying Authority to obtain digital signature certificate or to obtain license to issue certificates 72 Breaching confidentiality of electronic documents to which a person has access | Imprisonment upto 2 years or with a fine upto Rs. 1 lakh or with both |
| Section 73 | Publishing digital signature certificate with false particulars | Imprisonment upto 2 years or with a fine upto Rs. 1 lakh or with both |
| Section 72 | Breaching confidentiality of electronic documents to which a person ahs access. | imprisonment upto 2 years or with a fine upto Rs. 1 lakh or with both. |
| Section 74 | Creating, publishing or making available a digital signature certificate for any fraudulent or unlawfull purpose | imprisonment upto 2 years or with a fine upto Rs. 1 lakh or with both. |

**Section 75 of IT Act, 2000**

**Offence or contravention committed outside India which reads as:**

1. Subject to the provisions of sub-section (2), the provision of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

2. For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**The Information Technology Act, 2000** has a separate chapter on Offences i.e. Chapter XI. Now, it will be pertinent to discuss the provisions of this chapter.

**Section 65 of the IT Act, 2000 reads as below:**

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

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and program analysis of computer resource in any form."

The offences relating to cyber world can be done in two ways: one, by the human being alone such as obtaining the password and using it in an unauthorised way, two, by the human beings using software and some computer such as sending computer virus. In the later type, the crime can be investigated by detecting the computer from which, the virus originated or was sent and subsequently using the same as the evidence. Even in the former case, the computer and the phone number which is used to use the password in an unauthorised way have to be detected or used as evidence. Thus, here the computer becomes as crucial for investigation as the weapon of crime becomes in a murder case. If the weapon of crime for example the Pistol which fired the killing bullet is very crucial in investigation relating to a murder case: the bullet of that pistol is cross checked with the bullet found in the body of the victim; the finger prints on the pistol are examined to establish the killer. Similarly, the computer from which the computer virus emanated becomes crucial for the investigation here. It is necessary, therefore, that the computer be identified with the computer source code. The authenticity and integrity of the computer

source code has to be maintained fully. Section 65 of the IT Act, 2000 is an effort to ensure the same.

**Section 66 of the Information Technology Act, 2000 reads as below:**

"(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 upto three years or with fine which may extend upto two lakh rupees, or with both."

"Hacking" as defined in the Information Technology Act has got three ingredients: one, the intention to cause or knowledge that he is likely to cause wrongful loss or damage to the public or any person; two, the act of destroying or deleting or altering any information residing in a computer resource or of any information residing in a computer resource or of diminishing its value or utility or affecting it injuriously by any means and, three, the effect. The point to be noted here is that the intention to cause wrongful loss or damage is not the essential ingredient of the offence. Even if the intention is not there, the offence may be committed. Simply, the knowledge that he is likely to cause wrongful loss or damage by that act makes it a punishable offence under this section of the Act. But an act of causing wrongful loss or damage by that Act makes it a punishable offence under this section of the Act.

The third ingredient of the Act, i.e. the effect is a point pondering about. Suppose A attempts to wrongfully damage B's computer intentionally but since B has installed such a software in his computer as to protect it from the damage and also acquaint him of such an attempt, his computer is not damaged, rather he gets to know that A had attempted unsuccessful but intentionally to cause damage to his computer. So, can B file an FIR against A and if yes to what effect. Section 66 (2) of the IT Act makes the act of hacking punishable but not the attempt of hacking.

Further there is yet another issue related with this section. Can hacking be committed by an act affecting computer resource belonging to the person who commits the act, or to that person and others jointly? Section 66(1) of the Act clearly states that the wrongful damage may be to the public or any person. The term "any person" in my opinion includes the person who commits the offence himself as well.

Article 67 of the Information Technology Act, 2000 reads as below:

**67. Publishing of information which is obscene in electronic form** —Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons

who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to One lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to ten lakh rupees.

Here the word "or if its effect," "likely" and "tend to" are noticeable which bring into the facet of the law attempts relating to the offence in my opinion.

**68. Power of the Controller to give directions**.— (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

**69. Directions of Controller to a subscriber to extend facilities to decrypt information.—(**1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

**70. Protected system.—**

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

**71. Penalty for misrepresentation.—**Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**72. Breach of confidentiality and privacy**.—Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**73. Penalty for publishing Digital Signature Certificate false in certain particulars**.—(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; Or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revoca-tion.

(2) Any person who contravenes the provisions of sub-section (1)- shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**74. Publication for fraudulent purpose.—**Whoever knowingly creates, publishes or otherwise makes available a Digital publication for Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**75. Act to apply for offence or contraventions committed outside India**.—(1) Subject to the provisions of sub-section (2) the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**76. Confiscation**.—Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or

regulations made thereunder has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

**77. Penalties and confiscation not to interfere with other punishments.**—No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

**78. Power to investigate offences**.—Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

# CHAPTER 11 : CONCLUSION

Lastly I conclude by writing that “Thieves don't seem to be born, however created out of opportunities.”This quote specifically reflects this surroundings associated with technology, wherever it's dynamic in no time. By the time regulators come back up with preventive measures to safeguard customers from innovative frauds, either the surroundings itself changes or new technology emerges. This helps criminals to search out new areas to commit the fraud. laptop forensics has developed as an essential tool for enforcement. however within the digital world, as within the physical world the goals of enforcement are balanced with the goals of maintaining personal liberty and privacy. Jurisdiction over cyber crimes ought to be standardized round the globe to create swift action attainable against terrorist whose activities are adorable security worldwide. The National institute of justice, technical social unit digital proof are a number of the key organization concerned in analysis.

Cyber Crimes has empowered the average person to explore and question the structure of our society and those that benefit from the way it is operated. Fundamental issues arise from cyber criminal exploration. We must decide how, as a human being, how we wish to deal with these issues. We must decide as a society which direction that the new technology will go, what ends we hope to achieve, and what the limits on its use should be. There is no need to stop the technology, but we must decide what direction we want the technology to take, and what rules will govern its use. We must do this now, before the technology starts dictating the rules to us, before it’s too late to make the changes in the basic structure without destroying the whole concept.

# Bibliography


**Websites**

- http://cci.gov.in/
- http://www.academia.edu/
- http://www.hg.org/
- http://www,jstor.org/

**Books**

- Cyber laws By Justice Yatindra singh
- Cyber Crime By R.K. Suri and T.N. Chhabra
- Intellectual Property Rights (IPRs) :TRIPS Agreement & Indian law by E.T. Lokganathan
- Law relating to IPR by V.K. Ahuja

**Journals**

- International Journal of Cyber Crimiminology, Vol.8 Issue 1,January-June 2014.
- Cyber Times International Journal of Technology and Management,Vol.6 Issue 2,December 2013.