CHAPTER 3: CYBER CRIMES

1. INTRODUCTON

In today's era, Internet is the most advance mode of communication. Civilization standing at the forefront of the new millennium is facing a new from of crime called cyber crime. Cyber crime is probably the most commonly used terminologies of the modern time. The birth of Internet and its rapid growth has led to the evolution of new forms of trans-national crime known as "cyber crimes".

The most important feature of Internet is that, it completely ignores geographical boundary [1]. A person by sitting at any corner of the world can communicate with other person without disclosing his identity. The strength of the Internet is - fastest communication at cheapest rate. The Internet and its rapid growth, has raised many challenges not only for the governments but also for trade and commerce and individuals around the world [2].

However, it is unfortunate that Internet has its darker side too. Many of the characteristic features of Internet like, low cost, easy to use and fastest means of communication also gives rise to new forms of crimes like fraudulent scams, child pornography, hacking, and introducing viruses. Conventional law enforcement mechanism fails to resolve these new kinds of issues. It is felt that the new form of legislation is required to combat cyber crimes. The new millemium is witnessing a new form of crime, which can be done through Internet. At the outset it is worth mentioning that in some form the crimes committed through INTERNET differs from the conventional crimes. As Internet is decentralized, person can commit crime from anywhere in the world. Again it breaks the information into little parts called 'packets' due to which it becomes difficult to find the rout through which the information will be traveling. Further, the impact of wrongdoers act would be in altogether different country. In such

cases, as laws of different countries are not all together same, it becomes difficult to catch-hold the defendant.

2. FUNDAMENTAL PRINCIPLES OF CRIMINAL LIABLITY

Now before discussing various kinds of Cyber crimes, let us take a short trip to the basics of the Law of Crimes i.e. Indian Penal Code 1860. We must not forget that Indian Penal Code (hereafter IPC) nowhere defines anything like cyber crimes. The reason is at the time the act was drafted there was nothing like computer.

But at the same time we must also consider that before Information Technology Act was enacted it was IPC, which was applicable to all types of cyber crimes. Not only this but the provisions of the IPC will still be applicable where the IT Act is silent as to particular offence, which can be committed through Internet.
Now let us go back to the basics - The fundamental principle of criminal liability is laid down in the maxim – 'actus non facit reum nisi mens sit rea'. It means that, 'an act by itself will not amount to offence unless it is done with guilty intention'. Thus the criminal liability of the wrongdoer can be fixed provided following two essentials are satisfied:
- Actus reus i.e. Act
- Mens rea i.e. guilty mind

Now the question is whether these principles of criminal liability could be applicable to Internet crimes. The word 'actus reus' means any 'act', or 'deed'. It also includes 'omission to do' or 'not to do' something. It may be said as any physical result of human conduct. According to Smith and Hogan, Criminal Law – 'such result of human conduct as the law seeks to prevent'.

This element of actus reus can be clearly identified when there are Cyber crimes. The reason is a cyber crime requires certain act of the wrongdoer. For example, an attempt to make computer function etc. In all such cases there is bound to be some act on the part of wrongdoer.

Another important principle of criminal liability is 'mens rea' [3] – which means guilty mind. The essential feature of this principle is that, the wrongdoer must have been aware that what act he is committing is not permissible by law.

Again this element can also be identified in case of Cyber crimes – i.e. one cannot commit cyber crime unless he is well versed with technological aspects. Thus the person who commits that act would be well aware of what he is doing and what will be its impact. Any layman who is new to technological aspect of the computers cannot commit cyber crimes. Thus both the essential principles of criminal liability are present in case of Internet crimes. So in cases where IT Act is silent the substantive provisions of IPC can be applicable provided these two aspects (i.e. actus reus and mens rea) are taken care of.

3. DEFINITION OF THE TERM "CYBER CRIME" AND ITS SPECIAL CHARACTERISTICS

The term cyber crime is no more new to the Netizens. Now before discussing various kinds of cyber crimes and the legal provisions to curb it at both national and international level, we must first understand - "WHAT IS CYBER CRIME".
At the outset it is worth mentioning here that there is no perfect definition of cyber crime. The subject is still growing and therefore it is not possible to give the precise definition of the term.

Offences committed via Information Technology have taken within its orbit any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer system. Various terms are used (and misused) to define cyber crime. For present purpose, we may define cyber crime as, - a criminal offense that has been created or made possible by the advent of computer technology, or a traditional crime, which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime.

Within this broad definition lie two distinct sub-categories: Computer Crime and Computer-related Crime.

Firstly one may say that, Computer Crime involves the use of a computer as the primary instrument to facilitate the commission of crime. These crimes usually include the unauthorized:
- use, access or damage to a computer system;
- taking, copying, altering, deleting, or destroying computer data or programs;
- denying computer services to an authorized user;
- introducing viruses into any computer or system;
- misuse of someone else's Internet domain name.

Secondly one may say that, Computer-related Crime involves the use of a computer to commit a crime and/or as a repository of evidence related to the crime. Generally, this includes traditional crimes that have been transformed by computer technology such as:
- Internet auction fraud (primarily thefts);
- criminal threats;
- stalking (cyberstalking);
- threatening or annoying electronic mail;
- distribution of child pornography;
- online gambling;
- fraudulent credit card transactions;
- fraudulent application for goods or services; or,
- identity theft.

Cyber crimes have been on a rise at an alarming rate. In a survey by the CSI (March 12.2001), 85% of respondents, primarily large corporations and government agencies, detected computer security breaches within the last 12 months. 64% acknowledged financial losses due to computer breaches 35% where wiling and/or able to quantify their financial losses, which amounted to $377,828,700 in financial losses up from $265,589,940 in 2000. The most serious financial losses occurred through theft of proprietary information [4].

The importance of recognizing these two distinct categories is critical, in that they require varying levels of investigative skill. Specifically, computer crimes require a much higher degree of technical knowledge than computer-related crimes.

Thus the term "cyber crime" encompasses a variety of different crimes, ranging from crimes specific to computers (such as hacking and cracking) to "normal" crimes, which can be perpetuated by use of a computer (like extortion and solicitation).

Before we discuss in detail different types of cyber crimes, we must understand the special characteristics of cyber crime:

- Cyber crimes are committed with the use of Technology. They are the outcome of technology, and thus cyber criminals are very good with technological aspect of Internet.
- Secondly, Cyber crime operates and affects in no time. Thus it is committed very efficiently.
- Further cyber crimes know no geographical boundaries. A person can hack computer from any nook and corner of the world. He can commit cyber fraud by sitting in USA and may see its effect some where in Gujarat.
- Again, invisibility is the great attribute of the Internet. Except the cyber criminal who is physically outside the cyberspace, all components of cyber criminality from preparation to execution, takes place in the cyber world. Thus, degree of risk in cyber criminality is extremely low in comparison to other traditional crimes such as murder, rape and kidnapping.
- The offence of cyber crime will cause loss, which can be unimaginable. It can destroy a web site, which has been created and maintained with huge investments.

4. 'CYBER CRIME' UNDER INFORMATION TECHNOLOGY ACT 2000

Even the Information Technology Act 2000, which deals with certain offences relating to Internet, does not define cyber crime. How ever for the sake of proper understanding we may divide the term into two parts: -

Firstly – we may limit the definition of cyber crimes, as only those crimes that are specifically covered by The Information Technology Act 2000. In such case it will include crimes like Hacking, Cyber pornography, Virus launching etc. Thus, the first aspect specifically deals with new offences. We may also consider this as, a narrow definition of cyber crime.

Secondly – we may define the term broadly to include, "all unlawful acts that are done by computer. Here a computer may be either a instrument or a target or both". This we may say would be the broadest definition of the term cyber crime. It includes any act committed on or with the help of Internet. This broad definition widens the scope of the act to considerable extent. Thus offences that are not specifically covered by the IT Act 2000 will fall under this category. For example fraud, cheating, defamation etc.

Let us take some example to understand the definition:
1). If a person with the help of internet cheats another person, then he will be liable for cheating as per the provisions of S.420 [5] of Indian Penal Code. Here the provisions of IT Act will not be applicable, as it does not deal with the offence of cheating. Nevertheless this wrongful act will fall into the broad definition of cyber crime. This is due to the fact that the wrongdoer has committed crime via Internet.
2). We can take yet another example to understand the broad meaning of the term. For example a person commits the offence of Cyberstalking (in brief it means harassment of person by sending threatening e-mails). As Cyber stalking is not covered by IT Act, it would not amount to offence under that Act. Even in Indian Penal Code there is no specific provision for harassment, however we may apply S.503 of IPC, which deals with criminal intimidation. The section has following essentials:

Threatening the person with an injury –

a). to his person or property

b). to the person or reputation of any one in whom that person is interested

the threat must be with the intent –

a). to cause alarm

b). to cause the person to do any act which he is not legally bound to do

c). to omit to do any act that the person is legally entitled to do.

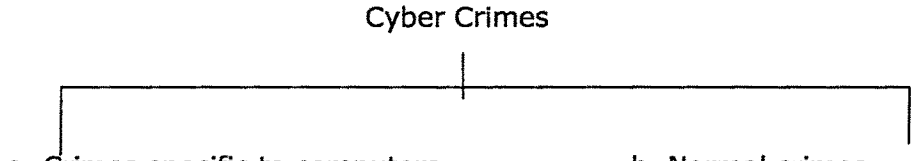
The offence of criminal threats requires a person in whom he is specifically interested to be threatened. There must be intent to cause alarm to the former by a threat of injury. The intent itself might be complete, though it could not be effect. But the existence of the interest seems essential to the offence, as also and equally to the attempt to commit the offence, since otherwise the attempt would be to do something not constituting the offence [6].

Section 503 of the IPC specifically refers to the effect, of the threat that is intended to have upon the mind of the person threatened. In any act of stalking, the person being stalked will suffer injury in the form of mental distress. Therefore, the act of Stalking may be covered under Section 503 of the IPC.

The Information Technology Act provides for and punishes only certain Cyber offences and is not exhaustive of all cyber crimes. For offence where IT Act is silent, but the commission of the offence includes the use of Internet it will attract the provisions of Indian Penal Code and the act will be called cyber crime. Though the IT Act 2000 defines and punishes only a few cyber crimes, it recognizes that there are other crimes which can be committed via Internet and there the provisions of Indian Penal Code 1860 will be applicable.

5. DIFFERENT KIND OF CYBER CRIMES

Cyber crimes can be classified into two broad categories:



a. Crimes specific to computers
-Hacking/Cracking
-Launching of Virus
-Cyber stalking/Harassment & email abuse
-E-mail spoofing
-Security related crimes
-On-line gambling

b. Normal crimes
* Cyber Defamation
* Fraud
* Child Porn.

Now let us discuss in detail different types of Cyber crime and the legal provisions at both national and international level to curb it: -

5.1 Hacking and Cracking

What we mean by "hacking and cracking" are actually the offenses against the privacy, integrity, and availability of computer data. The term is now no more new to the Netizens. Among all the crimes that takes place on the information superhighway, Hacking is the gravest cyber crime ever known. Hacking in simple terms means an illegal intrusion into a computer system and/or network.

According to The New Hacker's Dictionary, a hacker can be defined as:

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
- One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
- A person capable of appreciating hack value.

- A person who is good at programming quickly.
- An expert at a particular program, or one who frequently does work using it or on it.
- An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
- One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
- A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. The correct term for this sense is cracker.

There is an equivalent term to hacking i.e. cracking [8], but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They have a desire to destruct the computer program. Some hackers commit the offence of hacking for personal, such as to steal the information relating to credit card, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information, which is critical in nature. It is really a dreadful feeling to know that a stranger has broken into your computer system without your knowledge and has tampered with your confidential information.

There are various kinds of hackers [9]. The term is used to describe all of these like – Code Hackers who are very good with the various operations of the computers, Phreakers who are having in-depth knowledge of the Internet, and Cyberpunks who are good with cryptography. They do hacking at times for fun, to damage the business of competitors etc. Motive behind Hacking are greed, power, publicity, revenge, adventure, desire to excess forbidden information, destructive mindset etc. Hacking is the most serious crime of all cyber crimes. In countries like USA, millions of rupees are spent to prevent hacking. Losses due to this crime also goes in million. The worst part of hacking is that it creates threats among corporate world that net is insecure. It will make e-

commerce costlier as huge amount would be require to install software's to guard against hackers. If we want e-commerce to succeed, hacking must be stopped at any cost. Usually, Hacking is done by means of sending the virus to the computer.

Before we discuss the provision in the IT Act which deals with hacking, we shall for the sake of understanding divide the definition in two parts:

Firstly, the term refers to those irresponsible acts of individuals who will do it for the sake of fun or to damage the business of the competitors. This people are interested to stretch the limits of the program instead of learning only that, which is necessary. For such people it a hobby to explore the details of the programmes.

Secondly, in its most popular terminology it refers to breaking into a computer system.

Indian Position

Section 66 of the IT Act 2000 deals with Hacking. The Act has taken a unique approach to defining the term 'hacking'. Hacking is usually understood to be unauthorized access of computer systems and networks. However, Indian law has chosen to define hacking in relation to information.

The section reads as under:

S. 66. Hacking with computer system:

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

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

Essential ingredients of the offence of hacking are as follows.

Firstly, there must be either
- an intention to cause wrongful loss to any person. Thus innocent act of individual, where by he commits the offence will no be covered under S.66 of the Act,
- knowledge, that wrongful loss or damage will be caused to any person

Secondly, information residing in a computer resource must be either
destroyed,

At the outset it is worth mentioning that the IT Act has not defined the term "destroy". According to the Oxford dictionary destroy means "to make useless", "cause to cease to exist, nullify". According to the Law Lexicon destroy means to demolish or reduce to nothing. Destroying information also includes acts that render the information useless for the purpose for which it had been created. Information in a computer resource is stored in files (e.g. document files). Thus to make out an offence under this clause it would be necessary to prove either one of the following:

- That the contents of the file have been changed so as to make the file useless for the purpose that it was initially serving. (E.g. A file contains the resume of Mr. B. If this file is so altered that it is no longer the resume of Mr. B, then such file has been destroyed.)
- That the contents of the file or the file itself have ceased to exist due to the acts of the hacker.
- That the contents of the file have been removed.
- Deleted,
  It means, to make no longer effective by crossing out or removing. In the context of information in a computer, this would mean removing a file or the information contained in such file. However, whether the offence of hacking would be made out if a deleted file has been subsequently

retrieved (from the recycle bin for example) is a matter to be settled by the courts in due course.

- Altered, or
  This means that there is some change in the position or contents of the file.
- Diminished in value or utility,
  This we may understand appropriately by way of an example. Suppose a high quality graphic image is stored in .psd format (using a software called Adobe Photoshop). This format supports high quality for the image. If an unauthorized person changes the format from .psd to .bmp (a bitmap format which does not support high quality images), then this person is said to have diminished the value or utility of the information.

The definition of hacking is so wide that numerous cyber crimes would be included under the ambit of hacking. Some of these are virus attacks leading to loss of information, data diddling, and Internet time theft. Further, Section 66(2) of the IT Act provides for imprisonment up to 3 years and / or fine up to Rs 2 lakh as a punishment for hacking. So to prove the offence of hacking, both wrongful act and mensrea (guilty mind) must be proved. Thus the innocent act of the individual, whereby he commits the offence without intention, it will not amount to hacking. Further, compensation by way of damages can also be claim under Civil Procedure Code whereby it wont be required for the plaintiff to prove that defendant did the wrongful act with guilty mind. Among all kinds of cyber crimes, Hacking is the most dangerous one. The reason is it affects the creditability of the Internet. Here also the decentralized nature of the Internet and our dependency over computers play an important role. A person residing in other country can commit an offence of hacking by his acts. It is simple to execute also. Government websites are the hot targets of the hackers due to the press coverage, it receives.

Hacking is defined very widely in the IT Act. However the term nowhere discuss anything of "breaking into computer systems". On the other side it talks of – "destroying or deleting or altering any information residing in computer system...diminishes its value or utility or affects it injuriously by any means.

Thus hobbies of hacking, planting of virus, defacing etc will be covered within the wide amplitude of the term. This word makes the definition very wide...even launching of virus will fall under this definition (S.66).

On Jan. 25, 2001 two men of a local computer-teaching institute were arrested under section 66 of the IT Act for the offence of hacking. S.420 of IPC for illegal gain and S.379 for theft and S.426 for Mischief for introducing the programme to Net users. The programme, which copied down passwords, database and files, had enabled the senders to hack secret files of banks, business and e-mails (10). It is not that there have been very few cyber crimes in India. The inadequacies in the Act have failed to bring Net criminals to court.

Measures taken by the USA to combat the crime of Hacking

One may be surprised to know that more than 60% of the sites on the World Wide Web are located in the USA. To curb the menace of hacking the US Govt. has enacted various stringent legislations. We shall now discuss some important features of these legislations: -

The Computer Fraud and Abuse Act deals with the issue of unauthorized access in the US legal system. The legislation was first enacted in 1984, revised in 1994 and last amended in late 1996 [11]. It makes certain activities designed to access a *federal interest computer* illegal (a federal interest computer is defined to include: a computer used by a financial institution, used by the United States Government, or one of two or more computers used in committing the offence, not all of which are located in the same State). Spinello (2000) states that these activities: "May range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command".

Further the Act prohibits the use of unauthorized access to computers to commit the following seven crimes:

1. Espionage
2. Access Unauthorized Information
3. Access Non-Public Government Computer
4. Fraud by Computer

The provisions of the Act protect the confidentiality of proprietary information and make it crime to "*knowingly access a computer without or in excess of authority to obtain classified information*". In addition, it is also a crime to access any *protected computer* without authorization and as a result of such access to defraud victims of property or to thoughtlessly cause damage (a protected computer is defined to include those used by the government, financial institutions, or any business engaged in national or international commerce). Stealing classified information, perpetrating fraud, and / or causing damage, for example, destroying files or disabling an operating system is viewed as trespass and is a federal crime. Spinello (2000) argues that the only strict trespass provision of the statute protects computers used on a full time or part time basis by the government from unauthorized access, even if no damage is done and no information is stolen [12].

The Computer Misuse Act, 1990 (United Kingdom)

Until the Computer Misuse Act, 1990 was passed, offenders could have been charged under Section 13 of the Theft Act which dealt with, stealing electricity. However, the charge was artificial as the quantity of electricity involved was so small and indeed may not have been measurable. Other alternatives were misuse of the public telecommunications networks contrary to the Telecommunications Act, 1984. Forgery, criminal damage or the offence of intentionally intercepting a communication in the course of its transmission by means of a public telecommunications system contrary to the Interception of Communications Act, 1985 was common [13]. In 1988 the House of Lords decided contrary to the long held assumption in the UK that hacking was illegal in the United Kingdom. Their Computer Misuse Act of 1990 provides for two offences relating to unauthorised access to computers. The first offence is "Unauthorised Access to Computer Material". This offence is committed when a person causes a computer to perform a function with the intent to secure unauthorised access. If a person therefore gains unauthorised access to a computer system while knowing that he does not have authorisation, he commits the crime. The second crime created by the Computer Misuse Act is "Unauthorised access with the intent to commit or facilitate Commission of

further offences". This crime basically prohibits a person from gaining unauthorised access if he has the intention to commit a further crime [14].

Now if we compare Section 66 of the Information Technology Act we can see that the section is worded very broadly to include even launching of the virus. Thanks to our legislatures for using such a foresight, and defining the term widely. As the law is still evolving in this area, it seems that our legislatures by using broad words in the definition has acted wisely to meet the future contingencies.

Measures taken by Canada to combat the crime of Hacking

In 1985 Canada passed the Criminal Law Amendment Act. This amendment added Section 342.1 to the Criminal Code of Canada (hereafter referred to as the Code) as well as adding Subsection (1.1) to Section 430 of the Code. The Criminal Law Improvement Act 1997 added Subsection (d) to Section 342.1(1).

The most relevant sections of the Code are:

342.1 (1) Every one who, fraudulently and without of right,
(a) Obtains, directly or indirectly, any computer service,
(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly,
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

430. (1) Every one commits mischief who willfully
(a) destroys or damages property;
(b) renders property dangerous, useless, inoperative or ineffective;
(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.
Will be held liable for imprisonment for 10 years and fine.

We are standing at the forefront of new millennium. Law enforcement agencies around the word are trying there best to curb the crime of Hacking. Laws with deterrence are the only measure to curb the menace of Hacking, besides relying upon the new technology. India, by enacting Information Technology Act 2000 had answered the call of time and responded rightly to the changing technology and growth of society. Undoubtly S.66 of the IT Act, which defines Hacking, is widely drafted, but we will surely reap its benefits in the days to come.

5.2 Launching of Virus on Internet

Virus is a program created by human agent to alter or destruct any digital information. They are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They are usually programmed to alter or delete the data stored into computer. It has its history in John von Neumann's studies of self-replicating mathematical formula in 1940's. The first famous case of computer virus names 'in the wild' occurred in October 1987.

It is a program or piece of code that is loaded in your computer without your knowledge and runs against your wishes. Viruses can also duplicate themselves. All computer viruses are manmade. A simple virus may make a copy of itself repeatedly and may quickly use all available memory in the computer. This may also lead the system to a halt. Some dangerous viruses are capable of transmitting itself across networks and bypass even the security systems. Thus, the term is now no more new to the Netizens, especially after the attack of 'I Love You" bug. It is said that, one Philippine undergraduate

created the "I Love You" virus. On May 2000 this virus became the world most prevalent virus. It replicate itself as it went, and infected millions of computers, erased data, including precious photo and music files, and paralyzed electronic communications for countless people from members of Parliament to offices on Capitol Hill, to major corporations like Ford and Lucent [15]. It was more damaging virus ever, several times more than Melissa virus, which cost the estimated loss of 80 million dollars. Such is the menace of viruses – and the amount of loss has doubled each year. Trojan Horse, Logic Bombs and worms are all cousins of virus, having special destructing features [16].

Today, viruses affect thousands of computers every year. Users are spending several hundred millions on anti-virus software's. At times even software company will launch virus first and then they will put their anti-virus product in market to earn good money.

Measures taken by India to curb the crime of Virus Launching

Section 43 C of The Information technology Act 2000 provides that:

"If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network ...introduces or causes to be damaged any computer contaminant or computer virus into any computer, computer system or computer network...shall be liable to damages by way of compensation not exceeding one crore of rupees to the person so affected".

Further S.47 deals with the following factors to be taken into account while determining the quantum of compensation:

- the amount of gain of unfair advantage
- the amount of loss caused to a person
- the repetitive nature of the default

Further the Explanation to S.43 defines the word 'damage' which means to destroy, alter, delete, add, modify or rearrange any computer resource by any means. "Computer damage" has been defined as 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. "Computer contaminant" has been defined as any set of computer instructions that are designed - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network, or by any means to usurp the normal operation of the computer, computer system, or computer network.

The section imposes monetary liability of damages by way of compensation to the victim. This liability will be imposed irrespective of wrongful intention, negligence or innocently. It must be understood that introduction of a virus is a serious offence. Where a wrongdoer introduces a computer virus or computer contaminant with the intention or with a knowledge that his act may cause damage, and by such introduction deletes or alters any information residing in a computer resource or diminishes its value, then his act shall also amount to Hacking u/s 65 which is made punishable with imprisonment upto 3 years or with fine which may extend up to Rs. 2 lakh, or with both.

At the out set it is worth mentioning here that the section 43 of the IT Act provides only monetary liability...it does not talk about corporeal punishment. It is submitted that along with monetary liability some corporeal punishment must also be provided so that it will carry a deterrent effect.

Section 425 of Indian Penal Code (Mischief)

Further ---the act of planting virus can also fall under Section 425 of Indian Penal Code, which deals with the offence of Mischief. Section .425 of IPC says: "Whoever, with the intent to cause or knowing that he is like 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 effects it injuriously, commits 'mischief'.

Explanation I - 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 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 II – Mischief may be committed any an act affecting property belonging to the person who commits the act, or to that person and others jointly.

Let us try to understand the definition by way of some examples: -
- Mr. P voluntarily throws a ring belonging to Mr. Q into a river; with the intention of causing wrongful loss. Mr. P has committed an offence of mischief.
- Mr. A introduces water into an ice-house belonging to Mr. Z; and thus causes the ice to melt, intending wrongful loss to Mr. Z. Mr. A has committed the offence of mischief.

Following essentials if, satisfied would constitute the offence of mischief:
- Destruction of property, or any change in the property, which may destroy or diminish the value of the property.
- Any wrongful loss or damage to the public or to any person by any of the above mentioned acts.
- The aforesaid acts are committed with intent to cause wrongful loss to the public or to any person.

If one compares cyber crimes with traditional land based crimes, it can be found that it has posed number of new challenges to the global legal community. Since it is difficult for the law enforcement agencies to combat cybercrimes, it is not only the job of government, but it is also the responsibility of the global virtual community to put there all efforts to curb this menace.

In 1985 Canada passed the Criminal Law Amendment Act. This amendment added Section 342.1 to the Criminal Code of Canada (hereafter referred to as the Code) as well as adding Subsection (1.1) to Section 430 of the Code. The Criminal Law Improvement Act 1997 added Subsection (d) to Section 342.1(1).

430. (1) Every one commits mischief who willfully
(a) destroys or damages property;
(b) renders property dangerous, useless, inoperative or ineffective;
(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property. Will be held liable for imprisonment for 10 years and fine.

In India it seems, our legislatures while enacting IT Act had used broad terminology. Thus the word "computer damage" and "computer contaminant" as defined in S. 43 are would enough to including even Hacking within its ambit.

5.3 Cyber stalking, Harassment and E-Mail abuse

Cyberstalking

Internet is a new frontier. It is wide open to both exploitation and exploration. The hard fact is that, there are no police on the Information Superhighway. No one is there to protect you or to lock-up virtual bandits. This lack of supervision and enforcement leaves users to watch out for themselves and for each other. Unfortunately, cyberspace remains wide open to faceless, nameless con artists that can carry out all sorts of mischief.

Although there is no universally accepted definition of Cyberstalking, the term may be used to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking may be defined as the repeated acts of harassment or threatening, such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. However, much depends on the course of conduct of the stalker.

There are two kinds of Stalkers – Online & Offline. Both have desire to control the victim's life. Majority of them are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires.

Offline vs. Online Stalking -- A Comparison

Major Similarities

Majority of cases involve stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace.
Most victims are women; most stalkers are men.
Stalkers are generally motivated by the desire to control the victim.

Major Differences

Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyberstalkers may be located across the street or across the country.

Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim (e.g., impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening messages back to the victim "author"). Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim.

Online stalkers can make claims difficult for law enforcement officials to pursue by perpetuating the harassment in anonymity. The stalker could also use methods, which cannot be saved (such as sending messages over programs such as MSN Messenger) or traced (like posting a controversial statement on a message board under the victim's e-mail address). Again, online harassment is very similar to offline stalking. Stalkers are generally motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end. In most cases, the stalker and the victim had some sort of relationship, which the victim ended. Due to the vast amount of information

available online, stalkers can gather very easily vital information about their victims. (For example while chatting on the net one can see the profile of the individuals, and can know their e-mail address and even from which country he/she is located). The anonymity of the Internet also provides new opportunities for would-be cyberstalkers. A cyberstalkers true identity can be concealed by using different ISP's or by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an e-mail or other electronic communication.

An existing problem aggravated by new technology

Although online harassment and threats can take many forms, Cyberstalking shares important characteristics with offline stalking. Many stalkers - online or offline - are motivated by a desire to exert control over their victims. As with offline stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women. The fact that Cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to Cyberstalking. While there are many similarities between offline and online stalking, the Internet and other communications technologies provide new platform for stalkers to pursue their victims.

A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will

have the intended effect on the victim, but the cyber stalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender. Anonymity leaves the cyber stalker in an advantageous position. Wrongdoer could be in another state, around the corner, or in the next cubicle at work. He may be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. In addition, some perpetrators, armed with the knowledge that their identity is unknown, might be more willing to pursue the victim at work or home, and the Internet can provide substantial information to this end. Numerous websites will provide personal information, including unlisted telephone numbers and detailed directions to a home or office. For a fee, other websites promise to provide social security numbers, financial data, and other personal information.

How do they operate?

a) They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place. If the stalker is one who knows the victim as his colleague or former friend then he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

b) Secondly, the stalker may post this information on any website which is related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons. This will lead to havoc in victims life.

c) People of all kind from nook and corner of the World, who come across this information, may start calling the victim at her residence or work place and may also ask for sexual services or relationships.

d) Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

e) Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
f) Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

With Internet the communication has became faster and cheaper at cost. Further Internet provides the platform to communicate with the world at global level. Not only this but it provides the freedom of speech and expression to every man who is using Internet today. Cyber stalking and e-mail abuse has become very common. Women's are more vulnerable to this now a day. For example a man and a women meet in chat room and they developed relationship. Then after sometime the relationship ends up and the man will start harassing the women by sending abusive e-mails - almost hourly. After sometime the woman starts receiving the mails from unknown person asking for sex. To make the things more badly that man will post her telephone number and address on the net asking the people that go and see her for "good time".

Measures taken by India to curb the crime of Cyberstalking

Indian Information Technology Act 2000 is silent on this issue. The best way to stop electronic harassment is to make laws prohibiting it. Unfortunately Information Technology Act 2000 is silent over this issue. Until any such law is enacted, it is possible to prevent them by making small efforts like awareness and education to all Internet users. In India, also people must have faced problem of stalking and harassment, but unfortunately it has not been reported.

Indian Penal Code

Even Indian Penal Code doesn't provide any provision that specifically deals with harassment. But for Cyberstalking we can take into consideration Section 503-507 of IPC. Section 503 of IPC deals with Criminal Intimidation. It says...
"Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or cause that person to do

any cat which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation".

- Thus for the offence of criminal intimidation what is require is that either a person or another in whom he is specifically interested to be threatened. There must be intent to cause alarm to the former by a threat to him of injury to himself or to the latter. The intent itself might be complete, though it could not be affected. But the existence of interest seems essential to the offence, as also and equally to the attempt to commit the offence, since otherwise the attempt would be to do something not constituting the offence.

Thus the section has following essential features:
- threatening the person with an injury:
  to his person, reputation or property
  to the person or reputation of any one in whom that person is interested,
- further the threat must be with the intent:
  to cause alarm
  to cause the person to do any act which he is not legally bound to do so
  to omit to do any act that the person is legally entitled to do.

Further S.507 says:
"...Whoever commits the offence of criminal intidimitatl0n by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence by the last preceding section".

Thus the section clearly refers to the effect, which the threat is intended to have upon the mind of the person threatened. In any act of stalking, there is a clear "injury" to the person being stalked in terms of mental distress. Therefore this section provides for stalking and also harassment.

Cyber stalking has become rampant on the net, but still surprisingly the IT Act fails to take not of it. If e-mail is innocently worded, it would not be treated as criminal intimidation punishable under the Indian Penal Code 1860. Therefore it is submitted the Cyberstalking should have been defined and made punishable under the IT Act 2000. Cyberstalking legislation has been passed in the US so as to penalize and keep a check on this menace. (Kindly see -PAEDOPHILES ON THE PRAWL. Lady Chat friend kidnaps 16-yr-old boy...Mumbai (India) 20/11/2000 From www.Chalomumbai.com (Mid-day) By: Bhupen Patel)

Measures taken by the USA to curb the crime of Cyberstalking

The U.S. Attorney General defines cyber stalking as "the use of the Internet, e-mail, or other electronic communications devices to stalk another person." Stalking is considered to be harassing or threatening behavior that a person engages in over and over again. Most statutes require that the stalker make a believable threat of violence against the victim.

While most protection is offered through state legislation, there are a couple of important tools to combat cyber stalking on the federal level. 47 U.S.C. Sec. 223 criminalizes stalking via interstate or foreign communications; this misdemeanor is punishable by up to two years in prison. 18 U.S.C. Sec. 875(c) makes it a federal crime to transmit "in interstate or commerce any communication containing any threat to kidnap any person or any threat to injure the person of another." Further, President Clinton signed the Interstate Stalking Act in 1996, which makes it a crime to travel to another state to injure or harass another person. (18 U.S.C. Sec. 2261A) [17]

Cyberstalking is a relatively new challenge for most law enforcement agencies. The first traditional stalking law was enacted by the state of California in 1990 - less than a decade ago. Since then, many law enforcement agencies have trained their personnel on stalking and established specialized units to handle Cyberstalking cases. Nonetheless, many agencies are still developing the expertise and resources to investigate and prosecute traditional stalking cases; only a handful of agencies throughout the country have focused attention or

resources specifically on the Cyberstalking problem [18]. Federal law provides a number of important tools that are available to combat Cyber stalking. Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce - thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet [19]. The Interstate Stalking Act, signed into law by President Clinton in 1996, makes it a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's family in a reasonable fear of death or serious bodily injury. See 18 U.S.C. 2261A. Although a number of serious stalking cases have been prosecuted under Section 2261A, the requirement that the stalker physically travel across state lines makes it largely inapplicable to Cyberstalking cases [20]. Finally, President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity. While this new statute provides important protections for children, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes. (See: 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY Vice President Al Gore)

We can see that the position in the USA is more forward looking. The recent emergence of electronic harassment has prompted the states like Michigan, Alaska, and Oklahoma to pass legislation making e-mail or Internet communication subject to criminal laws that prohibit harassing or stalking. There are citizens groups like Women Halting On-line and even a branch of the Guardian Angles called Cyber angles have formed to help people who complain about harassment. (Source: www.usdoj.gov/criminal/cybercrimes)

Cyber Defamation

Along with Cyberstalking, the cases of CYBER DEFAMATION have also increased on the Internet. The most common meaning of the defamation is injury done to the reputation of the person [21]. Internet defamation may be similar to defamation in other forms: such as defamation published in a newspaper or broadcasted on television. It has, however, several features that make it unique and possibly devastating to the subjects of it [22]. They are:

Size:

The Internet is an unparalleled source of information. It is comprised of billions of publicly available pages, covering every subject known to man, and its size is increasing every day. In September of 2002, it was estimated that 605.6 million [23] people worldwide were Internet users. This is clearly a larger potential audience than any newspaper or cable station has ever attracted. As the U.S. Supreme Court stated in ACLU v. Reno, when comparing the Internet to more primitive forms of communication:

"[A]ny person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox." Reno v. ACLU, 521 U.S. 844, 870 (1997) [24].

Continuous Publication:

The Internet, as a means of publication, has more "staying power" than many other forms of communication. This means that unlike a cable or radio broadcast, which airs most programs only one time, information that is put on the Internet will stay there until it is taken down by an information content provider. Moreover, it is different than most magazines or newspapers in that they have a definite publication date, to which courts treat every copy of a magazine as published on that day.

Anonymity:

The Internet is also a unique medium for communication in that so many of its speaker's are anonymous. In chat rooms, on message boards, or even in personal emails, most people communicate in these forums using a pseudonym,

such as "john_doe2001," which masks their true identity. Although using such a mask may inspire some users to speak more freely, it may also be the reason that defamation on the Internet occurs, as people are not afraid of the consequences from their speech. In U.S. the Supreme Court has held that the right to speak anonymously is part of the First Amendment right to freedom of speech. Buckley v. Am. Const. Law Found. 514 U.S. 334, 341 (1995). Although the Court addressed anonymous speech in the form of leaflets in that case, it follows that a similar right attaches to Internet speech [25].

Liability:

The Internet as a medium for communication is also unique because of who can be held liable for defamatory messages. In traditional tort law, a newspaper or other publisher of defamatory material may be a possible defendant if it publishes that material. An Internet Service Provider ("ISP"), however, cannot.

Before discussing the issues of who the proper defendant is in an Internet defamation case, determining his geographic location is an important issue, that if overlooked could mean the end of any lawsuit against him. The concern here is that in order for a court order to be binding on a defendant, the court must have proper subject matter and personal jurisdiction over the defendant. In order for a state to properly assert jurisdiction over a defendant, the defendant must meet the "minimum contacts" test. This test requires that the defendant has "purposefully availed" himself with contacts in the state sufficiently so that the Constitution is not offended by the state court asserting jurisdiction over the individual. *See* Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945); Hanson v. Denckla, 357 U.S. 235 (1958). (I have discussed this case at length in chapter of Jurisdiction)

Moreover, suits arising from activities on the Internet create another twist in the jurisdiction analysis due to the worldly nature of the Internet. It may not be fair, however, for a plaintiff to assert jurisdiction anywhere in the world over a defendant merely because Internet sites can be accessed anywhere. Thus, courts are tending to apply a sliding scale analysis for evaluating minimum contacts based on online activity. This test, as seen in Zippo Mfg. Co. v. Zippo

Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997), considers both the quantity and quality of the contacts to determine if jurisdiction over the defendant is proper. A defendant who merely places a defamatory remark online—contrasted with an operator of a commercial web site—lies at the lowest end of the spectrum, and likely a court will deem jurisdiction over the defendant proper only in his home state, and not in every state where these remarks can be read. Thus, it becomes increasingly important for the plaintiff to properly identify the author of the defamatory material so that his location can be determined, or he may lose his suit on jurisdictional grounds. In one instance, one state would not allow a plaintiff to collect a $25,000 judgment in its state that it said was improperly granted—based on improper jurisdiction—by another state court. (Griffis v. Luban, 646 N.W.2d 527 (Minn. 2003) [26].

Identifying the Defendant

More often than not, defamatory remarks are written online with either no identifying information of the speaker, or at best, a pseudonym. When this is the case, a plaintiff who wishes to pursue legal action against the writer may face huge hurdles just in getting simple, identifying information such as the name and address of the author. The first step a plaintiff will take is to ask the ISP for this information. Typically, the ISP collects personal information about its users in its routine practices, but due to privacy concerns, the ISP may only be willing to divulge this information upon a court order to do so. The ISP is under no legal obligation to tell the user if they are going to comply with a subpoena request, but it is the policy of most to do so. For instance, MSN Privacy Policy states:

MSN may access and/or disclose your personal information if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect and defend the rights or property of Microsoft, including its MSN family of Web sites; or (c) act under exigent circumstances to protect the personal safety of users of Microsoft, its web sites, or the public [27]. Similarly, Yahoo informs its users that their information may be given out to:

respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.

Before complying with a request, such as a subpoena seeking the identifying information, the ISP will likely inform the user of the request, and it will be the user's responsibility to fight it. Several cases have arisen surrounding the circumstances under which an ISP must comply with these subpoena requests. The general trend of courts in US sis to require the plaintiff to set forth a *prima facie* defamation action against the alleged defendant and to attempt to notify the defendant of the subpoena request (by using the email address, for instance, if this information is known). If the plaintiff can meet this burden, a court will likely order the ISP to comply with the subpoena request for information [28].

Measures taken by India to curb the crime of cyber defamation

At the outset it is worth mentioning that Indian Information Technology Act 2000 does not deal with the cyber defamation and therefore we have to rely on Indian Penal Code. Internet defamation can take place on net, through any one of the following communication avenues: email, web site postings, chat rooms, etc. The target of the "cyber smear" may be an individual person, a corporate entity, a governmental entity, or something else. As the Internet increasingly becomes a reference source of information, Internet defamation has the potential to do more and more harm. Internet, which provides virtually all freedom to express ones views, provides free ground to make defamatory statements also. This can be done via, e-mail messages, mailing lists and newsgroups (this are discussion foras)

Meaning of Defamation under IPC

Now let us see the meaning of Defamation under Indian Penal Code. The common meaning of defamation is injury done to the reputation of a person. Defamation is a criminal offence under Section 499 of IPC, which consists of following essentials:

- making or publishing an imputation concerning any person,

-the imputation is made with the intention of causing harm to, or knowing or having reason to believe that such imputation will harm the reputation or such person. The imputation is made by words, which are either spoken or intended to be read, or by signs or by visible representations.

The Explanation 4 to S 499 provides that an imputation cannot be said to harm a persons reputation, unless that imputation directly or indirectly in the estimation of others lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful. Section 499 also provides exceptions whereby the imputation will not be an offence. They are, an opinion in good faith, publication of substantially true report, statement that are true and are made in public good. The punishment for defamation as provided in section 500 of IPC is simple imprisonment for a term, which may extend to two years, or with fine, or with both.

Law of defamation, by providing exceptions, seeks to balance the democratic freedom of speech and expression for public good with the malicious and dishonest imputations harming the reputation of a person. As the interaction via Internet grows, the law of defamation will have to be frequently invoked. Anonymity on the Internet together with speed and global access at very low cost, have provided an opportunity to criminal netizen having violent minds to threaten and intimidate others, which is also punishable under IPC. Criminal intimidation by anonymous communication – concealing the name, which is becoming rampant on the Internet, is punishable with imprisonment for a term, which may extend to two years in addition to the punishment for criminal intimidation (Section 507 of IPC).

The Internet provides a medium to the Netizens to communicate at the global level. It not only facilitates but also promotes the freedom of speech and expression to common man who can use computer. Further, Internet promotes democracy by providing a very efficient, easy and cost-friendly medium to all its users to communicate globally, and also provides many forums such as chat rooms etc for Netizens to voice their views freely.

Though Internet promotes the most important democratic right – the freedom of speech and expression, which is guaranteed under our Constitution of India by Article 19(1)(a), it is also being misused.

The ugly and criminal abuse of the Internet is coming to light even in India. Some time back, an Engineering and Management graduate who was facing prosecution for harassing his wife for dowry was caught sending obscene e-mails in his wife's name to several of her relatives, friends and other in a bid to harass her further and thus was arrested by the Delhi Police. The modus-operandi allegedly used by him was to create a fake e-mail account in the name of his wife and then send e-mails to people giving a false impression that they were being sent by his wife. These e-mails allegedly contained pornographic material, extremely vulgar language and asked people to chat with her on a given chat site. The police arrested him and registered a case for defamation, criminal intimidation and acts intended to insult the modesty of women, under section 500, 506, and 509 respectively of Indian Penal Code [29]. This case is just a tip of an iceberg. There are many web sites committing the offence of defamation, criminal intimidation and insulting the modesty of women. Defamation and harassment through Internet is becoming rampant each day and threatens to be a major cyber crime in the future.

In many cases of e-mail abuse, criminals are targeting women for harassment. Sometime back, the Delhi police arrested one Manish Kathuria an Engineer and a MBA degree holder, who posed himself as the wife of his former boss. He posted her telephone number on a chat room and asked netizen to get in touch late night. The alleged motive was to seek revenge because the accused apparently believed that the husband of the victim, who was his ex-boss, was responsible for dismissal of the accused from his previous job. The victim, named Ritu Kohli, started receiving obscene calls at Delhi from As far as Dubai and Bahrain. The victim smartly found out the name of the chat site and logged on herself and chatted with the accused, pretending to be a man. Subsequently, a complaint was lodged with the Crime Branch. The Internet protocol address of the accused was found to be connected with the telephone number of the accused. The accused was thus arrested [30].

Offences as aforesaid amount to defamation of the victim and criminal intimidation. Insulting the modesty of a women or intruding upon her privacy is punishable with simple imprisonment for a term, which may extend to one year, or with fine, or with both. (S.509 of IPC). However, since S.509 of IPC does not cover 'written words' within its ambit, e-mail abuse for such purpose would not be covered under the said provision. It is submitted that, either section 509 of IPC should be amended to include written words or a separate offence should be incorporated in the IT Act 2000.

Measures taken by the USA to curb the crime of cyber defamation

According to Restatement (Second) of Torts 559 (1997) a communication is defamatory if;

"[T]ends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."

Although the First Amendment protects freedom of speech as a fundamental right in US, it is not an absolute right. The U.S. Supreme Court has identified defamation as an exception to the fundamental right of freedom of speech, meaning states may regulate or prohibit defamation. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 268-72 (1964). ("Whatever is added to the world of libel is taken from the world of free debate."). Additionally, defamation is classified as a tort, and state law regulates it [31].

According to RESTATEMENT (SECOND) OF TORTS § 563 (1977).

There is no master list of defamatory words. Instead, each case is a fact-heavy, totality of the circumstances determination of whether the statement was false and understood as defamatory by its audience. Babb v. Minder, 806 F.2d 749, 758 (7th Cir. 1986) [32]. How the communication is understood, however, is not a completely subjective question. Whether a statement is capable of being defamatory is a question of law, rather than fact, and a court will only apply reasonable meanings to statements.

Prior to 1996, the US courts followed traditional defamation law in holding that an ISP, like a publisher, can be held liable for defamation if it maintained any editorial control over the material that it provided. Stratton Oakmont, Inc. V. Prodigy Servs. Co., 23 Media L. Rep. 1794, 1799 (N.Y. Sup. Ct. 1995). In this way, the ISP was more than a "passive conduit," analogized to the newsstand that cannot be liable for such defamation, in the absence of fault. However, in the Stratton Oakmont [33] case, Prodigy was found to act more like a publisher because it reserved the right to remove any messages posted on its web site that did not comply with its Guidelines; this policy was an effort by Prodigy to upkeep a "family friendly" reputation. Thus, Stratton Oakmont could sue Prodigy for defamation, without every learning the identity of the author of the defamatory posting, who called Stratton Oakmont, "a cult of brokers who either lie for a living or get fired." The U.S. Congress changed this jurisprudence in the Communications Decency Act of 1996, Pub. L. No. 104-104 § 502 (e) (codified primarily in 47 USC § 230)

The CDA provided:

(c)(1): "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

An information content provider is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." [34]

Section (c) of the CDA, is entitled, "Good Samaritan" blocking and screening of offensive material, and at least one legal commentator has argued that it was meant to encompass only the Prodigy type situation where, in good faith, the provider was trying to screen offensive material. The courts, however, have interpreted section (c) very broadly, creating a large safe harbor for ISP's. In

Zeran v. America Online, 129 F.3d 327, *cert denied*, 524 U.S. 937, the court held that the CDA created a "federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." The court went on to state:

"Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content-are barred". (See: www.law.emory.edu/4circut/nov97/971523p.html)

It is worth mentioning over here that in India also the Internet Service Provides are immune from liability for the wrongful act of third party provided they prove that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. IT Act 2000

Other cases agreeing with this broad interpretation of the CDA:

- Ben Ezra, Weinstein, & Co v. America Online, Inc., 206 F.3d 980 (2000), *cert denied,* 531 U.S. 824 (2000) (holding that AOL was operating solely as an interactive computer service and could not be liable for allegedly defamatory information, written by a third party, that was posted on its site). (Source - www.legal.web.aol.cm/decisions/dldefame/bnezcoa.pdf)
- Blumenthal v. Drudge, 992 F.Supp 44 (D.C. Dist. Col. 1998) (holding that the ISP could not be liable for allegedly defamatory postings on its site, even though it had an employment contract with the gossip columnist that posted the materials). (Source - www.bluementhol_v_drudge.html)
- Stoner v. eBay, Inc., 56 USPQ2d 1852 (Cal. Sup. Ct. 2000) (holding that CDA provided federal immunity from any state law cause of action against an ISP for material it provided that was created by a third party).

At least one state has enacted a statute that echoes the protection offered by the CDA. Virginia Civil Statutes § 8.01-49.1. entitled: "Liability for defamatory material on the Internet," reads:

No provider or user of an interactive computer service on the Internet shall be treated as the publisher or speaker of any information provided to it by another

information content provider. No provider or user of an interactive computer service shall be liable for (i) any action voluntarily taken by it in good faith to restrict access to, or availability of, material that the provider or user considers to be obscene, lewd, lascivious, excessively violent, harassing, or intended to incite hatred on the basis of race, religious conviction, color, or national origin, whether or not such material is constitutionally protected, or (ii) any action taken to enable, or make available to information content providers or others, the technical means to restrict access to information provided by another information content provider. (See - www.jmls.edu/cyber/cases/start.htm)

Now if we look to section 79 of the IT Act which deals with the liability of ISPs, we can see the it is very rightly drafted. ISPs are just an intermediary, just like Telephone Company who provides facility of watching programmes on Televisions. The main function of the telephone company is to provide services of communication. How can a telephone company be held liable for what people are communicating on telephone? For example if Mr. A uses abusive language while talking on the phone with Mr. B, can we blame Telephone Company for that? Imagine the hardships that each telephone company had to undergo if they are to be held liable for what Mr. A has said to Mr. B. In the same way ISPs are just intermediaries, who provide access to information to the individual. Again they are providing services becoze they have charged for the subscription.

It is submitted that simply providing access may not constitute the doing of an offence. However, as Internet has its own demerits and that must be taken into account. Looking to this American On-line (leading ISP in USA) has taken initiative to block certain objectionable standard have also set high parameters for viewing the content. Thus, it is submitted that just because ISPs provides service facility of Internet they should not be held liable, provided they satisfy the other provision contained in S.79 of the IT Act.

5.4 Fraud on Internet

Internet fraud is said to be big business. But what is it, and does using the Internet create the fraud, or is the Internet just a different way of delivering 'traditional' fraud is different question. The term "Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme.

Fraud on the Internet constitutes about one-third of all cyber crimes ("Web Crime Statistics" on www. Intergov.org). Internet fraud has increased by a substantial 29% over the past year (Govt. reports sharp cyber-crimes rise" dtd 20-1-2000 on www.zdnet.co.uk). It is the most profitable business on the Internet. Infact, 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 on-line auctions and web-sites, misappropriation and transfer of funds, etc.

General techniques of fraud

The key to fraud is to persuade you that something is real, when in fact it is not. Once you accept that the fake is real then the fraud can take place - whatever it is. Whether you are buying the Eiffel Tower in Paris or the Taj Mahal in India (both are real and have been seen by millions of people) the essence is to believe the proposal that is put to you. Other types of fraud essentially persuade you to do something in the (wrong) belief that it should be done, or to accept something in settlement that proves to be without the value you were led to believe. But they all come back to the same thing - the fraudster has to persuade you that his vision of the world is the correct one.

The Internet is rather different. The biggest problem for the Internet user is that there is no physical reference to use. You can't go to a physical bookshop at www.amazon.com. You have to believe what the computer tells you, and that is the start of the problems.

There are many practical examples where people get the physical world wrong - they put their bank cards into fake ATMs and enter their PINs, they tell their friends and children their passwords (sometimes in public), they sign up to 'get rich quick' deals with people they don't know - so how well are we set up to handle the Internet world, where web sites are just exactly as good as their designer intended? The practical answer is just barely. The Internet is marketed as an anonymous zone. Information is free and users are anonymous. Now some of those features are desirable. When you go into a store it is the store that has to tell you who they are. If you pay with cash they will never know who you are and none of your legal rights are affected. They give you a receipt and you can check any of the details and get corrections made on the spot. If you want credit you have to tell them more about you, but not necessarily very much.

The Internet, by comparison, is anonymous whether you are the seller or the customer. For the seller it is as anonymous as they want to make it. This, of course, might be thought of as attractive to a fraudster. Stock manipulation, pyramid schemes, fraudulent business opportunities, offshore scams, are all types of cyber fraud. The Internet has made these all the easier with fraudulent web auctions, internet services, merchandise, pyramid and multilevel marketing schemes, business opportunities, work-at-home schemes, credit card issuing, sweepstakes, and book sales leading the way.

Financial Fraud

What we mean by "financial fraud" is fraud related to credit cards and bank accounts. This crime is closely related to that of identity theft, as cyber-criminals often borrow a person's identity to perpetuate these crimes, and hacking. On the other hand, there are other ways to reach a person's existing accounts. In some cases, a hacker has broken into a company (bank or

otherwise) or government computer to access pertinent information. In others, a criminal might install a program into a number of computers, which tracks a person's keystrokes. Braver criminals might set up a false e-Bay account or even a bogus company to trick unsuspecting victims into giving out their credit card numbers.

Auction Fraud

Auction fraud includes several situations:

Shilling: The seller arranges for false bids to be placed on items they have for sale, thus driving up both price and interest in the auction.

No show: The seller accepts payment but then fails to ship the item purchased or the goods shipped do not conform with what was advertised (goods are stolen or phony).

Shipping fraud: The seller overcharges for shipping to add on to the cost of the item in a way that the auction site does not take a percentage.

Review fixing: Some sellers "fix" their feedback by arranging fake sales so they or their friends can leave them positive feedback, thus encouraging others to put more trust in them.

Buyer collusion: One buyer makes a low bid, and a second buyer immediately makes a very high one. This ensures that no one else will bid. At the last minute, the second bidder retracts, allowing the first bidder to get the item for a very low price.

Buyer remorse: Buyers may refuse to complete their end of the deal by refusing to pay, causing a check to bounce, or stopping payment on a check.

Refund scams: A buyer claims that the item received is defective and that he wishes to receive a refund. Once the refund is secured, the buyer does not return the item.

At 64% of all reported Internet fraud, Internet auction fraud constitutes a huge amount of the complaints. (Estimate from the Internet Fraud Complaint Center) The six categories of items most frequently connected to claims of fraud are beanies (27%), video consoles/games/tapes (24%), laptops (18%), cameras/camcorders (14%), desktop computers (9%), and jewelry (8%). While beanies accounted for the most complaints, they resulted in the least amount of lost money; laptops took first place in that category [35].

Thus, Cyber Fraud is the fraud committed on the Internet. It is impossible to tell all forms of frauds on the Internet. According to on-line reports, For example, financial aid fraud was committed by some bogus companies posing as legitimate scholarship search services. These crooks often guarantee scholarships for up-front fees ranging from $10 to $400. Students that use these services often find that the information they've purchased is out of date, inapplicable, or simply useless. Almost no one ever receives the guaranteed minimum. Another example is Internet Related Services Scams, which are the most common fraud on the Internet.

The criminal posts to a newsgroup offering low cost web page storage and design. A businessperson considering going online sees the post and asks for more information. He or she hears tales of virtually unlimited disk space, incredible tech support, incredibly quick download speeds, registered virtual domain names and low costs. Thrilled, the business signs up, sending in the specifics for the page and maybe even getting sent a draft for proofing. But, no page ever shows up. The business has spent hundreds, maybe thousands of dollars and gotten nothing. Internet frauds also take many other forms like business opportunity fraud; Work-At-Home Scams; Loans on the Internet fraud; Job hunt fraud; medical fraud; sweepstakes fraud, and so on.

Thus Internet fraud is a form of white-collar crime. Internet fraud is a common type of crime whose growth has been proportionate to the growth of Internet itself. The Internet provides companies and individuals with the opportunity of marketing their products on the net. It is easy for people with fraudulent intention to make their messages look real and credible.

Measures taken by India to curb the crime of cyber fraud

The term "Fraud" has not been defined in the IT Act 2000 and therefore we have to go back to Indian Penal Code and Indian Contract Act. As per the IPC, a person is said to do a thing fraudulently if he dose that thing with the intent to de-fraud but not otherwise (S. 25 of IPC).

"Defraud" involves two elements; i.e. deceit and injury to the person deceived. As per section 17 of the Indian Contract Act 1972:

"Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:
- the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
- the active concealment of a fact by one having knowledge or belief of the fact;
- a promise made without any intention of performing it;
- any other act fitted to deceive;
- any such act or omission as the law specifically declares to be fraudulent.

Explanation – Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is, in itself, equivalent to speech.

This definition of "fraud" in the law of contract applies to civil and contractual relations between the parties and has no application to criminal law. Therefore, in India, for the purpose of criminal law, the expression "cyber fraud" would be misnomer and instead "cyber cheating" would be more relevant. The expression cyber fraud in the Indian context can be used for fraud under the law of contract and other civil laws. For claiming damages and compensation under the civil law, the expression cyber fraud would be appropriate while as a crime entailing corporeal punishment or fine, or both, "cyber cheating" will be more appropriate. All acts which amounts to cheating would be fraud but the vice-versa may not be true in all cases. It should not be misunderstood that for acts of cyber cheating, only punishment, corporal or fine or both, is provided and no claim for damages and compensation can be made. In all cases of cheating, a cause of action will also lie for damages under the civil law besides punishment under the criminal law. In the Indian Penal Code, there is no definition or offence of "fraud", though there are several provisions, which contain the ingredient of fraudulent intention, etc. The offence of "cheating" which is

popularly called "420" in India, is closest to fraud. "Cheating" has been defined as follows in the Indian Penal Code under section 415:
"Whoever by deceiving any person, fraudulently or dishonestly induces the person so deceived any property to any person, or to consent that any person shall retain any property, or intentionally induces that any person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to cheat.
Explanation – A dishonest concealment of facts is a deception within the meaning of this section.

Thus following are the essentials of the offence of cheating:
- A representation is made by a person, which is false, and which he knows is false at the time of making the representation.
- The false representation is made with dishonest intention of deceiving the person to whom it is made.
- The person deceived is induced to deliver any property or to do or omit to do something which he would otherwise not have done or omitted.
The punishment for cheating is with imprisonment, which may extend upto one year, or with fine, or with both (S. 417 of IPC)

Further, the offence of cheating by personation stands committed whether the individual personated stands committed whether the individual personated is a real or an imaginary person. S.419 of the IPC provides for punishment with imprisonment for a term, which may extend to three years or with fine, or with both.

Since the nature of Internet facilitates netizen to interact and transact without meeting each other physically, cheating by personation becomes easier and hence is likely to be an active e-crime in the future and these provisions will frequently come into play. Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, is liable to be punished with imprisonment for a term which may extend to 7 years with fine (s. 420 of IPC)

Major kinds of Internet Fraud

In general, the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the Internet are now appearing online (sometimes with particular refinements that are unique to Internet technology). With the explosive growth of the Internet, and e-commerce in particular, online criminals try to present fraudulent schemes in ways that look, as much as possible, like the goods and services that the vast majority of legitimate e-commerce merchants offer. In the process, they not only cause harm to consumers and investors, but also undermine consumer confidence in legitimate e-commerce and the Internet.

Here are some of the major types of Internet fraud that law enforcement and regulatory authorities and consumer organizations are seeing:

Auction and Retail Schemes Online. According to the Federal Trade Commission and Internet Fraud Watch, fraudulent schemes appearing on online auction sites are the most frequently reported form of Internet fraud. These schemes, and similar schemes for online retail goods, typically purport to offer high-value items - ranging from Cartier® watches to computers to collectibles such as Beanie Babies® - that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods) (36).

Business Opportunity/"Work-at-Home" Schemes Online. Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Identity Theft and Fraud. Some Internet fraud schemes also involve identity theft - the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain.
In one federal prosecution, the defendants allegedly obtained the names and Social Security numbers of U.S. military officers from a Web site, then used more than 100 of those names and numbers to apply via the Internet for credit cards with a Delaware bank. In another federal prosecution, the defendant allegedly obtained personal data from a federal agency's Web site, and then used the personal data to submit 14 car loan applications online to a Florida bank [37].

Market Manipulation Schemes. Enforcement actions by the Securities and Exchange Commission (38) and criminal prosecutions indicate that criminals are using two basic methods for trying to manipulate securities markets for their personal profit. First, in so-called "pump-and-dump" schemes, they typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly traded stocks or stocks of shell companies (the "pump"), then immediately sell off their holdings of those stocks (the "dump") to realize substantial profits before the stock price falls back to its usual low level. Any other buyers of the stock who are unaware of the falsity of the information become victims of the scheme once the price falls.
For example, in one federal prosecution in Los Angeles, the defendants allegedly purchased, directly and through another man, a total of 130,000 shares in a bankrupt company, NEI Webworld, Inc., whose assets had been liquidated several months earlier. The defendants then allegedly posted bogus e-mail messages on hundreds of Internet bulletin boards, falsely stating that NEI Webworld was going to be taken over by a wireless telecommunications company. At the time of the defendants' alleged purchases of NEI Webworld stock, the stock was priced between 9 cents and 13 cents a share. Ultimately, in a single morning of trading, NEI Webworld stock rose in 45 minutes from $8 per share to a high of $15 5/16, before falling, within a half-hour, to 25 cents per share. The defendants allegedly realized profits of $362,625 [39].

Second, in short-selling or "scalping" schemes, the scheme takes a similar approach, by disseminating false or fraudulent information in an effort to cause price decreases in a particular company's stock. For example, in one recent federal prosecution, a man who described himself as a "day trader" allegedly posted (more than 20 times) a bogus press release falsely stating that a major telecommunications- and Internet-related company, Lucent Technologies, Inc., would not meet its quarterly earnings estimates. The day trader allegedly traded approximately 6,000 shares of Lucent stock the same day that he posted the bogus press release. The false reports allegedly drove the stock's price down 3.6 percent and reduced Lucent's market value by more than $7 billion.

Other Investment Schemes: Other types of fraudulent investment schemes may combine uses of the Internet with traditional mass-marketing technology such as telemarketing (40) to reach large numbers of potential victims.
In a federal prosecution in San Diego, a major fraudulent scheme used the Internet and telemarketing to solicit prospective investors for so-called "general partnerships" involving purported "high-tech" investments, such as an Internet shopping mall and Internet access providers. The scheme allegedly defrauded more than 3,000 victims nationwide of nearly $50 million.

Credit-Card Schemes: Some Internet fraud schemes, which appear to be variations on the online auction schemes described earlier, involve the use of unlawfully obtained credit card numbers to order goods or services online.
One widely reported and intricate scheme, for example, involves offering consumers high-value consumer items, such as video cameras, at a very attractive price (i.e., below the price set at legitimate e-commerce Web sites). When a potential consumer contacts the "seller," the "seller" promises to ship the consumer the item before the consumer has to pay anything. If the consumer agrees, the "seller" (without the consumer's knowledge) uses that consumer's real name, along with an unlawfully obtained credit card number belonging to another person, to buy the item at a legitimate Web site. Once that Web site ships the item to the consumer, the consumer, believing that the transaction is legitimate, then authorizes his credit card to be billed in favor of the "seller" or sends payment directly to the "seller."

As a result, there are two victims of the scheme: the original e-commerce merchant who shipped the item based on the unlawfully used credit card; and the consumer who sent his money after receiving the item that the "seller" fraudulently ordered from the merchant. In the meantime, the "seller" may have transferred his fraudulent proceeds to bank accounts beyond the effective reach of either the merchant or the consumer.

Since February 1999, when the US Department of Justice established its Internet Fraud Initiative, the federal government has been expanding its efforts to combine criminal prosecution with coordinated analysis and investigation as part of a comprehensive approach to combating Internet fraud. The Dept. of Justice has begun to bring a number of criminal prosecutions throughout the country against individuals and groups engaging in various types of Internet fraud.

5.5 E-Mail spoofing

There are two terms with which Netizens are familiar now-a-days. These are; communication via electronic mail: email "spamming" and email "spoofing". Email "spamming" refers to sending email to thousands and thousands of users. It is similar to a chain letter. Spamming is often done deliberately to use network resources. Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. "Email spoofing" refers to email that appears to have been originated from one source when it was actually sent from another source. Individuals, who are sending "junk" email or "SPAM", typically want the email to appear to be from an email address that may not exist. This way the email cannot be traced back to the originator.

Email spoofing is the practice of changing your name in email so that it looks like the email came from somewhere or someone else. For example Mr. Ashok has an e-mail address – ashok@yahoo.com . His enemy Mr. Kiran spoofs her e-mail and sends obscene messages to all his acquaintances. Since the e-mails appear to have originated from Mr. Ashok, his friends could take offence and

relationships could be spoiled for life. This type of crime can also cause monatory damage. Spoofing is generally used by spammers as a first defense against people finding out who they are. It's also used by general malcontents to practice mischievous and malicious behavior.

There are number of possible reasons why people send out emails spoofing the return address: sometimes it is simply to cause confusion, but more often it is to discredit the person whose email address has been spoofed: using their name to send a vile or insulting message. Sometimes email spoofing is used for what is known as "social engineering", which aims to trick the recipient into revealing passwords or other information.

Dealing with a Spoofed Email

There is really no way to prevent receiving a spoofed email. If you get a message that is outrageously insulting, which asks for something highly confidential, or it is just plain and doesn't make any sense, then you may want to find out if it is really from the person it says it's from. You can look at the Internet Headers information to see where the email actually originated. Remember that although your email address may have been spoofed this does not mean that the spoofer has gained access to your mailbox.

Thus, a spoofed email is one that appears to originate from one source but actually has been sent from another source. In an American case, a teenager made million dollars by spreading false information about other companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies to share brokers and investors who where infirmed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money. E-mail spoofing is global problem. The only way to control is strong reliance on the technology. Making efficient firewalls and developing software that can prevent the spoofing the mail is the only answer.

5.6. Pornography on Internet

There is no settled definition of pornography in a multi-national environment such as the Internet and cultural, moral and legal variations all around the world make it difficult to define 'pornographic content' in a global society. However, the production and distribution of child pornography on the Internet is illegal in the US, India and many other countries. The topic is discussed at length in another chapter.

5.7 Security related crimes

With the birth of Internet and its unprecedented growth, network security has become a major concern. The anonymous nature of the Net has made Netizens more vulnerable to the cyber crimes. Breaking into the computer systems has become common. Private confidential information has become available to the public. Confidential information can reside in two states on the network. It can reside on the physical stored media, such as hard drive or memory or it can reside in the transit across the physical network wire in the form of packets. These two information states provide opportunities for attacks from users on the internal network, as well as users on the Internet. Let us discuss some of them in brief:

Network Packet Sniffers

Network computers communicate by breaking the information into parts called as packets. Since these network packets are not encrypted they can be processed and understood by any application that can pick them off the network and process them. A third party can easily interpret the network packets and develop a packet sniffer. A packet sniffer is software that uses a network adapter card in a promiscuous mode to capture all network packets that are sent across a local network. A packet sniffer can provide its users with meaningful and often sensitive information such as user account names and passwords.

Password attacks

Password attacks can be implemented using several different methods like the brute force attacks, Trojan horse programmes. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts

to identify a user password or account. These repeated attempts are called brute force attacks.

Distribution of sensitive internal information to external sources: At the core of these security breaches is the distribution of sensitive information to competitors or others who use it to the owners' disadvantage. While an outside intruder can use password and IP spoofing attacks to copy information, an internal user could place sensitive information on an external computer or share a drive on the network with other users.

5.8 Internet gambling

According to 1998 statistics from the US Department of Justice, Internet gambling has proliferated with an estimated increase in revenue from US$300m in 1997 to US$651m in 1998 and an increase from 6.9 million to 14.5 million gamblers in the corresponding years. The reason for its proliferation is the instantaneous, round the clock access to online casinos and anonymous communication with operators. A major concern for the authorities is the massive manipulation of gambling odds and credit card fraud by such operators in addition to the impact that such online casinos have on minors and those with compulsive gambling habits.

In India The Information Technology Act does not specifically deal with this aspect.

6. STUDY OF FEDRAL LAWS IN USA

In the United States, cyber crimes are the focus of legislation adopted at both the state and federal levels. The U.S. Constitution establishes that federal legislation is appropriate only when federal intervention is required. While federal legislative authority can pre-empt the states' ability to legislate in a given area, it rarely does. It is therefore not unusual for federal criminal laws to overlap with state prohibitions that address essentially the same issues. Although there are model statutes, such as the Restatements, Uniform Acts and the Model Penal Code, that are drafted by private groups and offered to the states as examples, there is no formal mechanism at either the state or federal level which requires or even encourages states to adopt uniform, consistent

laws. Since 1984, Congress has pursued a dual approach to combating computer crime. The "Counterfeit Access Device and Computer Fraud and Abuse Law," Pub. L. No. 98-473, Title II, Chapter XXI, § 2102(a), 98 Stat. 1837, 2190 (1984) and all subsequent amendments address computer crimes in which the computer is the "subject" - that is, computer crimes for which there is no analogous traditional crime and for which special legislation is needed. The federal government's other approach to regulating computer crime has been to update existing criminal statutes in order to reach similar crimes involving computers.

Homeland Security Act of 2002

The Homeland Security Act involves a provision that calls for punishment of up to life in prison for electronic hackers who are found guilty of causing death to others through their actions [46].

Cyber Security Enhancement Act of 2002 **(Text of Sec. 225)** [47]

The Enhancement Act was added to the homeland security bill (above) on September 19, 2002, and establishes that hackers convicted of causing injuries to others could face prison terms up to 20 years under cyber crime provisions. Critics of the act question why the punishments are more severe for hackers than street criminals who commit assault or murder. "It's more severe than [punishments for] crimes committed with a knife or gun," said Chris Hoofnagle, legislative counsel for the Electronic Privacy Information Center, a nonprofit public interest research center in Washington.

USA Patriot Act of 2002

The USA PATRIOT Act [48] was enacted on October 26, 2001, in the wake of the September 11 terrorist attacks on America. This act significantly changes the landscape of computer crime laws and expands the authority of law enforcement to intercept electronic communications. Of most importance is the change, which the PARTIOT Act makes to 18 U.S.C. § 1030, the criminal statute prohibiting computer hacking. The law now covers computers located outside of the United States when used in a manner that affects the interstate commerce or communications of this country. It updates the definition of "loss" to ensure full costs to victims of hacking offences are counted. It also clarifies the scope

of civil liability. It further eliminates the current mandatory minimum sentence applicable in some cases.

Another provision amends 18 U.S.C. § 2702 to authorize providers of electronic communications services to disclose the communications (or records of such communications) of their subscribers if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires the immediate disclosure of the information. This section corrects an anomaly in the current law by clearly permitting a provider to disclose non-content records (such as a subscriber's log in records) as well as the contents of the communications in order to protect their computer systems.

7. SOME OTHER OFFENCES PROVIDED IN INFORMATION TECHNOLOGY ACT

Apart from the offences that we have discussed above, there are other offences and violations that have been provided in the IT Act. Section 65 of the Act provides for Tampering with computer source documents. It says. --

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

Further Section 68 deals with the power of the Controller to give necessary directions. The sections lays down that whoever fails to comply with the order of the Controller of Certifying Authority, will be punishable with imprisonment for a term not exceeding three years, or with a fine not exceeding Rs 2 lakh, or with both.

Section 69 empowers the Controller to direct any agency of the Government to intercept any information transmitted through any computer resource, if he is satisfied that it is necessary to do so in the interest of sovereignty and integrity of India. Every subscriber or person incharge of the computer resource shall

extend all facilities and assistance to decrypt the information and whoever fails to assist the agency in this regard shall be punishable with imprisonment for a term, which may extend to 7 years.

A person who unauthorizedly secures access or attempts to secure access to a protected system as declared by a notification in the official gazette by the appropriate Govt. shall be liable for punishment with imprisonment upto 10 years and shall also be liable for fine. (Section 70)

The Act also aims to punish a person for breach of confidentiality and privacy, with imprisonment for a term, which may extend to two years, or with fine, which may extend to Rs 1 lakh, or with both. (Section 72).

The law also provides for confiscation of any computer, computer system, floppies, compact disks, or other accessories connected with any contravention of the IT law. (Section 76)

Further it has been specifically laid down in the act that penalties or confiscation under the same shall not prevent the imposition of any other punishment to which the person accused is liable under any other law for the time being in force. (Section 77). For example S. 43 c of the IT Act deals with the offence of launching virus, will also amount to the commission of the offence of mischief under S.425 of the IPC, which is punishable with imprisonment for a term which may extend to two years, or with fine, or with both.

8. HOW CAN CRIMINAL JUSTICE SYSTEM OF WORLD CONTROL CYBER CRIMES

IT Act 2000, provides for the most prevalent and convenient method used in our country to deal with crime; i.e. deterrence. The general policy of our lawmakers has been to use deterrent punishments as a strategy for combating crime. The law enforcement agencies in WORLD have always relied upon third degree methods of investigation rather than the use of scientific methods.

Firstly, a sovereign country may enact a legislation to deal with online crime as it has done with other forms of crime for centuries. As a matter of fact, many countries have already gone this route and has legislated online crime on a national level.

The second option is to deal with it in an International context, and legislate it by way of multilateral treaties. Countries can therefore contract with each other on how to deal with online crime.
The third option available is to create an international organisation that can deal with online crime effectively.

9. WHAT CAN BE DONE?

Considering the nature of cyber criminality it seems that deterrence is the only answer to cyber crimes. Besides deterrent laws, these are the strategies, which may be adopted simultaneously to deal with the menace of cyber crimes: -
Since cyber crimes are committed by advance technology, the law enforcement machinery must be provided adequate training regarding the technological aspect of the Internet. A cyber police must be well conversant with the ins and outs of the technology. In this era of Internet, investigation will not start with guns but with technological weapons.

Another most important point is, as cyber crimes disregards the geographical boundaries, there have to be global co-operation among the nations of the world. We must not forget that we are dealing with the global disputes and therefore the efforts to curb this should be also at global level. We also need effective laws for extradition and their implementation. The existing extradition treaties ought to be strengthened by cooperation of the international community.

The most effective weapon to combat cyber crimes is strong technological backbone. We must adopt strong encryption and other security measures. We need better locks on computers and not on jails to prevent cyber crimes.
The IT industry must take-up the responsibility of protecting its own computer systems by using secure technologies. The Government should also take proper initiative to encourage the use of security technologies. It must facilitate R&D.
Further cyber crimes must be reported. Victim must come out to report the crime.

It is also important that easy identification of the Netizens can be a good way to curb cyber crimes. Of course, privacy concern should also be taken care of, but it must be realized that identification of the Netizens in certain areas, like cybercrimes is very much necessary. Identification should be permitted but at the same its disclosure should be regulated and be allowed in exceptional circumstances.

10. CONCLUSION

In conclusion, it is submitted that we are merely at the threshold of the technology revolution and the impact of cyber crime on the economy and security has not yet been fully comprehended. The change in technology has been frenetic for the last few years. Even for the computer savvy person, the change has been quite disconcerting. Bearing in mind the impact of cyber crimes and the fact that traditional criminal activities have been facilitated by such technological advancement, for e.g. more efficient mobilization of organized crimes, drug trafficking, prostitution and racketeering, it is respectfully suggested that we cannot relax our persistent efforts to police cyberspace and to establish effective cyber laws in order to enable us to master, harness and improve Internet technology for the good of society in the long run.

We must remember that cyber crimes are the most dangerous of all the crimes because the magnitude of loss it is causing goes in billions. Again it can be committed very easily, without disclosing the identity, from any part of the world. This will surely lead to difficulty while investigating, collecting evidence and successful prosecution. Once the Internet becomes an integral part of the daily life of even the common man, which is not very far away, cyber crime, if not checked, at right time would be destructive to the civilization itself. It is submitted that, the growth of the Internet should be directly linked with the growth of the protective technology. The growth of Internet would be of no use if cyber crimes are not checked at right time. Terrorism has became a global phenomena, and it needs to be remembered that we need to have global

approach towards combating the cyber crimes must also be at global level. Criminal justice systems of the world should come down at one platform to solve the burning problem. The Internet is analogous to the high seas. No one owns it, yet people of all nationalities use it. It would perhaps be ideal if unification of Internet laws could be so achieved so as to minimize the discrepancies in application of such laws. This is vital considering the growth of commercial activities on the Internet. Changes need to be made to the existing Information and Technology Act 2000 in order to combat the numerous problems caused by the Internet.

Footnotes

1. The message over the Internet is broken down in packets. Each packet will choose its own route to reach to the destination. This packet (letter) will travel by different route to reach the destination, which may be in the same country or in different country altogether.
2. Each minute, over five million e-mail messages are being sent around the world. While it took more than a century to install the first 700 million telephone lines, the next 700 million will be installed in less than 15 years – 300 million in China and India alone. In the same period, there will be 700 million new wireless subscribers. It is forecast that there will be 1000 new communication services providers worldwide within the next two years. (www.isc.org - statistical reports).
3. It is well settled principle of common law that mens rea is an essential ingredient of criminal offence. A statute can exclude that element, but it is a sound rule of construction adopted in England and also accepted in India to construe a statutory provision creating an offence in conformity with the common law rather than against it unless the statute expressly or by necessary implication excludes mens rea. There is a presumption that mens rea is an essential ingredient of a statutory offence; but this may be rebutted by the express words of a statute creating the offence or by necessary implication.
4. See Web statistics: www.belmontpress.com/statistics.htm
5. S. 420. of Indian Penal Code says: "Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or any thing which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine. – (See: Indian Penal Code by Ratanlal and Dhirajlal.)
6. See: Indian Penal Code – by Ratanlal and Dhirajlal

7. It is well settled principle of common law that mens rea is an essential ingredient of criminal offence. A statute can exclude that element, but it is a sound rule of construction adopted in England and also accepted in India to construe a statutory provision creating an offence in conformity with the common law rather than against it unless the statute expressly or by necessary implication excludes mens rea. There is a presumption that mens rea is an essential ingredient of a statutory offence; but this may be rebutted by the express words of a statute creating the offence or by necessary implication.
8. Crackers break into the computer system and destruct the operating system and its security. They do this as a favorite pass-time.
9. There are various kinds of Hackers. They are: - 1) Code Hackers who know computers inside out. They can make the computer do nearly anything they want it to do. 2). Cyberpunks are those persons who are good with cryptography. 3). Phreakers are the person who combines their in-depth knowledge of the Internet and the mass telecommunications systems.
10. Indian Express- Vadodara. dated 25-1-2001
11. See: Unauthorized cases - http://www.scit.wlv.ac.uk/~in7504/hacking.htm)
12. Ibid 11
13. Ibid 12
14. A more comprehensive overview of the Act can be found at following website: http://www.ja.net/CERT/JANET-CERT/law/cma.html
15. Times Magazine May 15, 200 The Attack of Love Bug
16. Worm: This is similar to a virus but does not attach itself to files or programs in a computer. This leaves it free to spread through a network on its own. Trojan horse: This is a program that performs malicious actions while pretending to do something else. It is similar to a virus but does not try to reproduce itself
17. Source: 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY Vice President Al Gore
18. Ibid 17
19. Ibid 18
20. Ibid 19
21. See: www.unc.edu/cources/2003/spribng/law/357c/001/projects - What is Internet Defamation
22. Ibid 21
23. See- www.nua.ie/surveys/how_many_online/index.htms
24. See – www.supct.law.cornell.edu/supct/html/96-51125.html
25. See- www.epic.org/free-speech/buckley_v_aclf.html
26. See- www.law.library.stste.mn.us/archive/supct/0207/c301296.htm
27. See- www.privacy.msn.com
28. See- www.privacy.yahoo.com/privacy/us/sbc/details.html
29. "Man held for sending porn e-mail messages in wife's name" in The Times of India, New Delhi – dtd 25-7-2000
30. "First cyber sex crime in Delhi"- The Hindu dated June 18,2000
31. Source – www.2bc.edu/~herbek/cases/nytvsullivan.html
32. See- www.loislaw.com
33. See - www.jmls.edu/cyber/cases/start.htm

34. See - www.jmls.edu/cyber/cases/start.htm
35.See: The Internet: A New Era for International Cooperation on Crime Control By Jeff Zexi - www.gsulaw.gsu.edu/law)
36.See-www.ftc.gov
37.See – www.usdoj/criminal/fraud/idtheft.html
38.See – www.sec.gov
39.See – www. usdoj.gov/usao/cac/pr/pr2000/003.htm
40.See – www.usdoj.gov/criminal/fraud/telemarketing/index.htm
41.See – www.thomas.loc.gov/cgi-bin/bdquery
42.See: www.jmls.edu/cyber/statutes/email.cal629_z.htm
43.See: www.legi.state.va.us/cgi_bin/legp504.exe
44.See: www.jmls.edu/cyber/statutes/email.cal629_z.htm
45.See - www.jmb.edu/cyber/statutes/email/nvsb13en.html
46.See- www.whitehouse.gov/deptofhomeland/bill/index.html
47.See –www.usdoj.gov/criminal/cybercrime/homeland_CSEA.html
48.See – www.epic.org/privacy/terrorism/hr3162.html