ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(7): 616-625
www.allresearchjournal.com
Received: 21-05-2017
Accepted: 22-06-2017

Smariti
LL.M., Net BPS Government Medical College Sonepat, Haryana, India

Correspondence
Smariti
LL.M., Net BPS Government Medical College Sonepat, Haryana, India

Classification of cyber crime

Smariti

1. Introduction

Crime involving high technology is going to go off the board was quoted by special agent Witen Tafyo of FBT. Cyber Crime is increasing leaps and bound. With the increase of Internet connectivity [1]. Keeping in mind. We can classify cybercrimes classification of cybercrime is very complex task because it is new spectacle of crime with even increasing and ever growing phenomenon.

There are several ways of classification of Cyber Crime.

Categories

1. Crime is the target as well as victim. For e.g.: hacking cyber theft cyber block mailing etc.
2. Crime is incidental to other crime Cyber pornography, harassment unlawful banking transaction & others.
3. Crime associated with the prevalence of computers which are also to be called as computer crime Software Piracy, counter fitting etc.

Donn [2] Parker identified four forms of computer abuse namely:-

1. Computer might serve as the victim of crime.
2. Computer might constitute the environment with in which a crime is committed
3. Computer might provide the means by which might is committed
4. Computer might symbolically be used to intimidate, deceive or defraud victims.

1.1 Classification of Cyber Crime

We can classify cybercrime as:-

2.1.1 Unauthorized Access
2.1.2 Cyber theft
2.1.3 Cyber hacking
2.1.4 Cyber Fraud
2.1.5 Cyber pornography
2.1.6 Cyber Terrorism
2.1.7 Cyber stalking
2.1.8 Flowing of virus
2.1.9 Violation of privacy
2.1.10 Spamming
2.1.11 Intellectual Property crime.
2.1.12 E-Mail spoofing
2.1.13 Computer Vandalism
2.1.14 Money Laundering
2.1.15 Data Diddling
2.1.16 Cyber Defamation
2.1.17 Paedophillia
2.1.18 Online Gambling
2.1.19 Sale of illegal Articles
2.1.20 Page–Jacking
2.1.21 Online security fraud.

1.1.1 Unauthorized Access

Knowingly and intentionally use or access without prevision or consent of the owner or possessor whole or any part of a computer systems, computer network to commit any cybercrime as denied above is unauthorized access. This is like criminal trespass committed in the real world.

Section 441 of the I.P.C define criminal trespass

"Criminal trespass: Whoever enters into or upon property in the possession of another with intent to commit all offence or to intimidate insult or annoy any person in possession of such property or having lawfully entered into or upon such property, unlawfully remains. There with intent thereby to intimidate, insult annoy any such person or with intent to commit an offence is said to commit 'Criminal trespass" the Computer fraud and Abuse Act 1984 was revised in 1994 amended in 1996 in the United States to prevent and control cybercrimes. Spinello (2000) states that these activities: may range from knowingly accessing a computer without authorization on exceeding authorized access to the transmission of a harmful component of a program, in for nation, code or command. This Act prohibits unauthorized access to computer to commit other crimes which include access of unauthorized information, access non-public Government computer and others. This Act Prohibits. Unauthorized access to information and perfect confidential information. That whoever knowingly accesses a computer without or in excess of authority to obtain classified information is guilty of unauthorized access even though no damage is caused or value of information is not reduced. Section 65 of the Information, Technology Act, 2000 in India Prohibits tampering with computer source documents and prescribes punishment.

1.1.2 Cyber Theft

The theft of information or identity e.g. name, date of birth, social security Number, credit card Number, password are increasing day by day in cyberspace with other cybercrimes. In the year 1988, 31st May, in the USA, in support of the Identity theft and Assumption Deterrence Act, the Generate Accounting office published a report called.

'Identity Fraud: Information on Prevalence, cost and Internet Impact is Limited'. The report stated that social security Number misuse is increased from 305 in 1996 to 1153 in 1997. Master card International Inc. and Visa U.S.A. Inc. stated that losses from their number banks were the $100 million dollars in a year. Master card stated that 96% number banks loses $407 million dollar for identity fraud in year 1997 only.

Most miserable fact is that victims of identity theft even most of the times do not realize that their identity has been stolen by someone else. Sometime at the times of further financing e.g. for home, for vehicle etc., they realize from lender that they do not have sufficient credit limit and therefore they become ineligible for loan for home, vehicle or otherwise.

Identity theft may be committed due to careless. Sharing of personal information and identities to international and dishonest stealing of digital information from home or public places. Sometimes we carelessly handle credit card and other confidential documents in public place and give information to others about card number security number, password etc. over phone which may be heard by potential criminal at the time of conversation and they may try to access those documents and commit identity theft. Not only in Public places, even at home or private places while we are using our computer or other devices and document we must do it very carefully so that others must not access it. The identity Theft and Assumption Deterrence Act was enacted on 30th October 1998 popularly known as. Identity Theft Act was passed to amend existing. Fraud and misuse Act to enhance penalties in related matter and to make provision suitable in contemporary social phenomenon to prevent and control Identity Theft or Cyber Theft.

Towards prevention, investigation and prosecution of identity theft seminars, workshops, conferences were held World Wide which proved strategies. Another possible challenge is to communicate victims to obtain basic information for investigation including losses and retreat if any. To achieve these goals law enforcement agencies require interaction with victims and witnesses so that they can make and improve their communication system and link bet" law Enforcement agencies and victims are helpful for victims as well as investigations to access case related information.

Cyber Theft may be governed under S/378 of Indian Penal Code, 1860

S/378 of Indian Penal Code

Whoever intending to take dishonestly any moveable property out of possession of any person without that person's consent, moves that property in order to such taking by the electronic means is said to commit of cyber theft is called cybercrimes this is like cyber theft U/S-378 of IPC

Moveable property according the electronic means is that computer, computer system and using of computer and other electronic means to theft of another computer resources.

1.1.3 Cyber Hacking

Hacking would means destruction or alteration of any information residing in a computer resource i.e. computer resource of tangible or intangible. Tangible assets include the hardware, components of the computer resources whereas intangible assets include information in the electronic form, magnetic or optical impulses.

Hacking is the most common form of cybercrime in these days. The reason why hackers indulge in this crime may vary from monetary gain to political interest or it may even be for the sake of shear thrill. Hacking may be different forms such as web-spoofing, e-mail bombing, Trojan attacks, virus attacks, password hacking etc. in simple words hacking means seeking of unauthorized access through computer network [3].

Web jacking as specify of hacking is nothing but force fully tacking over control of a website of someone else or the victim. The motive is usually ransom of attainment of some illegal political purpose.

E-mail bombing means sending large number of mails to the victim which may be an individual or a company to cause confusion and harassment.

Trojan is an unauthorized programme which gains control over another's system by representing itself as an authorized programme.

The administrator of any website has a pass word and a user name, then only he may use to upload files from his computer on the web server where his. Website is hosted. This password remains secret with the administrator. If a

hacker gets hold of this username e or password then he can pretend to be the administrator.

Computer hackers may affect the commercial website or e-mail systems thus paralyzing the entire business.

3.S/66 Inf. Tec. Act 2000

The terms of hacking as defined under Act seem somewhat similar to mischief as defined U/S 425 of Indian Penal Code, 1860:

"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 alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking."

Thus hacking signifies mischief with the computer resource. It is the mischief regarding destruction or resources. It is the mischief regarding destruction of alteration of any information residing in a computer resource and it is hacking with computer system i.e. using one computer to hack into another computer.

To brand any computer misuse as hacking would not only be fallacious but also against the spirit of the S-66 of the Act. It is important that fulfillment of all the ingredients as given in the aforesaid section are a must before an accused could be pronounced guilty of the offence.

1.1.4 Cyber Fraud

Fraud committed through computer, computer system, computer network or internet related communications are to be treated as cyber fraud. Any unauthorized access to commit fraud is to be treated as double crime in cyberspace one is unauthorized access which is similar to criminal trespass under s. 441 of the Indian Penal Code and another is commission of fraud after this unauthorized access.

Internet fraud can be committed through websites, e-mail junk mail, spamming, posting a message on an online bulletin board chat room is discussion, which is very difficult for the victims to identify whether the act in internet in fraudulent or actual fact.

S/25 of the Indian Penal Code, 1860 defines fraudulently that person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Section 66. Proposed Amendment as per Info. Technology (Amendment) Bill, 2006 include the terms fraudulently and dishonestly.

Illegal use or access of computer to cause wrongful loss to others property intentionally or knowingly by any input alteration, deletion on suppression of computer data base, computer system, computer programme, software etc. are also to be treated as computer related fraud.

The computer fraud and abuse Act, 1984 which prohibits using unauthorized access of computer to commit crimes these are:

1. Espionage
2. Access unauthorized information
3. Access of nonpublic Government computer
4. Fraud by computer.
5. Damage to computer
6. Trafficking in Passwords
7. Threats of damage a computer

The electronic market place offers consumers unprecedented choice and convenience, and it gives businesses of all kind low-cost access to a global consumer base. With these benefits, however, comes the challenge of ensuring that the virtual market place is a safe and secure place to purchase goods, services and digital information. As commerce on the Internet grows law enforcement agencies are observing a growing variety of fraudulent schemes that use the internet, either to communicate false or fraudulent representations of the prospective victims or to obtain value able information or resources necessary for the success of the schemes.

One form of internet fraud that is of particular concern is that of identify theft which generally involves obtaining data from individual consumers financial transactions on the Internet or elsewhere and lithe billing the consumer's credit cards for nonexistent transactions or services or using consumers personal data to conduct actual transactions that are billed to the consumers.

Other Internet Fraud schemes includes so called payment schemes ; entities that purport to be internet banks that offer above market rates for deposits; companies that promise to repair consumers' credit, but that to nothing after taking consumers' companies that purport to offer investments in none existent items, such as 'prime bank' securities or software to solve the Y2K problem; companies that are thinly traded on securities market or in fact are merely shall companies; and companies that fraudulently offer to sell Internet – related goods and services, or the collectible goods through online auction. Finally, some fraud. Schemes combine use of Internet websites with telemarketing. 'boiler rooms' to enhance direct contact with prospective victims.

1.1.5 Cyber Pornography

Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupt their mind set. A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment which may extend to imprisonment upto five year and liable to fine, which may extend to rupees one lakh [4] (S/67 of Information Technology Act. 2000). The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material in any electronic form.

It may be stated that child pornography constitutes a distinct category of cybercrime. This is committed by the lise of computer and the internet by its abusers to reach and abuse children sexually throughout the world at any place. The children are targeted and trapped by the abusers and they become their victims. Pedophiles explore this chance by providing their false identity on the internet and make contect with children in chat rooms or via e-mails where these children in chatted for giving their personal information. The pedophiles drag children to the internet for the purpose of sexual assault so as to use them as sex object. They attract children by providing them pornographic material. Indecent exposure is also covered in this category of cybercrime.

Nowadays internet has entered into our drawing room and even pocket through new technology and communication convergence e.g. computer, pocket PC, wireless, mobile phone, television etc. with internet connection. The demerits of the technological evolution is growth of crime rate in society e.g. child abuse, sexual harassment, digital

exploitation of child and women, video clips, use of smart camera or web camera for live sex or pornographic picture of girlfriend, school friend, actor, actress, teachers and other cybercrimes as well as other abuse and misuse. Enumeration are not exhaustive in Indian contemporary technological era. This problem is not only in India but rather the USA, the UK, Canada, Australia, Pakistan, China, Bangladesh and whole world is facing same problem.

4.S/67 of Inf. Tec Act 2000

The Indian Penal Code 1860, SS 292, 293 and 294 provide for limitations and prohibition of certain things which are obscene with one exceptional case. Section 292 prohibits sale, distribution, publication, export, import etc. of obscene books, pamphlets, papers, writing, drawings, paintings, representations and the like except justifications under this sections e.g. literature, art, learning, monuments, et. and prescribes punishments on first conviction with imprisonment for a term which may extend to two years and with fine which may extend to two thousand rupees, and on second conviction with imprisonment for a term which may extend to five years and also with fine which may extend to five thousand rupees.

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

1.1.6 Cyber terrorism

Cyber terrorism has domestic as well as international ramifications. It may be defined as the premeditated use of disruptive activities or the threat there of in cyber space with the intention to further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives, A cyber terrorist' may be defined as a person who uses computer system as a means to achieve any of the following objectives:-

(i) Putting the public or any section of the public in far: or
(ii) Affecting adversely the harmony between different religious, racial language or regional groups or casted or communities.
(iii) Covering or over a wing the government established by law
(iv) Endangering the sovereignty and integrity of the nation.

Every act done in pursuance of the above objective will be an act of cyber terrorism.

The term "cyber terrorism" is coined by a senior research fellow in California institute for security and intelligence, Mr. Barry Collin in 1980s composed two terms "cyberspace" and "Terrorism". The term "Terrorism" as premeditated, politically motivated violence perpetrated against non – combing targets by sub-national groups or clandestine agents, usually intended to influence an audience.

Information terrorism is the intentional abuse of a digital information system, network or component towards an end that supports or facilitates a terrorist campaign or action

Terrorists are addicted more to cyber war than to making bomb. Even for making bomb for conventional attack they are using Information and communication Technology for quicker and cheaper communication within groups and between groups. When the terrorist attacks the Government, Government activities or general people which are against national interest, it will be called cyber terrorism. In this sense we can interpret cyber hacking, breaking, cracking, flowing virus and objectionable materials, destruction, alteration, deletion of computer, computer programme, computer system, computer network of Government or Government agencies institutions, or general public which cause terror are to be treated as cyber terrorism.

Therefore, there are two prime concept of cyber Terrorism

(1) When terrorists us information technology to attract their audience by creating violence, through defacement of website, denial of service, attack, hacking, racking, tampering source code, flowing viruses etc. Where computer is used as target or weapon and which go against Government or national security.
(2) Another is terrorized use of information technology i.e. cyber pornography, cyber fraud, cyber theft, spamming etc. which causes terror or threat in the mind of people. Here the new technology is also tool of terrorism. Therefore, Cyber terrorism may be defined as use of computer as weapon or target to cause violence to population or which go against national interest and Governments computer system for the purpose of the explanation. Telephone, Mobile phones, wireless. Computer facilities are available almost everywhere in World. That is why terrorists are able to communicate with each other even being in remote area. They can control the entire group activities from remote area. Use of mobile phones and e-mail with internet use is increasing day by day among terrorist group as convenient means to communicate, control and monitor their groups. To avoid detections and investigations terrorists frequently use different cyber cafes. They are using remote controlled Improvised Explosive Devices to cause death and destruction. They are communicating with other terrorist group World Wide through internet.

1.1.7 Cyber stalking

In stalking persistant message are sent to unwilling mental torture. Sending of unsolicited e-mail or spamming is an infringement of might of privacy. Online harassment and threats may take many forms. Cyber stalking would occur with women who are staked by men adolescents and adult pedophiles. A cyber stalker does not have to leave his home to harass his targets and has no fear of physical avenge since he cannot be physically touched in cyber space.

A cyber stalker generally collects all the personal information about the victim such as name, age, family background, telephone or mobile numbers, workplace etc. He collects this information from the internet resources such as various profiles the victim may have filled in while opening the chat or e-mail account.

The menace of cyber stalking has spread like wild fire in India and many innocent women, girls and children are being targeted as its victim. The term is used in this report to refer to the use of the internet, e-mail or other electronic communications devices to stalk another person stalking generally involves harassing or threatening behavior that an individual engages in repeatedly. Such as person, appearing at a person home or vandalizing a person's property. Stalking laws require that the perpetrator make a credible threat of violence against victim; others include threats

against the victim's immediate family; and still other require only that the alleged stalker's course of conduct constitute an implied threat. While some conduct involving annoying or meaning behavior might of short of illegal stalking, such behavior may be preclude to stalking and violence and, should be treated seriously.

Online harassment and threats can take many from by be stalking, share important characteristics with offline stalking. Money stalkers, offline or online-are motivated by a desire of to exert control over their victim and engage in similar types of behavior to accomplish thus end. As with offline stalking, the available evidence suggests that the majority of stalker. Are men and the reported of their victim are women, although there have been reported cases of women cyber stalking men and of come- sex cyber stalking. In many case the cyber stalker and victim has prior relationship begin when the victim attempts of to break off the relationship. However, there are also have been many instance of cyber stalking by stronger. Given the enormous the amount of personal information available, through the internet, a cyber-stalker can easily locate the private information of about a potential victim with a few mouse clicks or key stroke.

The fact that cyber stalking does not involve physical contact may create the misperception that it is more begin than physical stalking. This is not necessary thus. As the Internet becomes an ever more integral part of our personal and professional lives, stalker can take advantage of the ease of communication as well as increased access to the personal information. In addition the ease of use and non-confrontational, impersonal and sometimes anonymous nature of internet communications and May remove, disincentives tee cyber talking. Whereas potential stalker may be unwilling or unable to confront the victim of person or on the telephone he or she may have little hesitation seeding of harassing or threatening electronic communication of to a victim. Finally, as with physical stalking online harassment and threats may be a preside to more serious behavior, including physical violence,

A cyber stalker may send repeated, threatening, or harassing message by the simple push button; more sophisticated cyber stalkers use programmed to send messages at regular or random intervals without being physically present at computer terminal. Each message- whether from the actual cyber stalker or others will have the intended effect on the victim, or but the cyber stalkers efforts is minimal on and the lack of direct contact between to the cyber stalker and the victim on can make it different for law enforcement to identify locate and arrest of offender.

1.1.8 Flowing of virus

Flowing of programmed through computer network by human agent such as virus, Trojan Horse, works, Logic Bombs of cause damage, alter, debate destroy computer, computer system, computer network, computer data base are also cybercrime. There are three types of viruses. They are popularly known as fill infectors through spread sheet programmed of games, boot, sector viruses through diskette or hard dies i.e., read into memory and exacted when a computer first start, and make versus, which depend on operating system and infect files and which contain data. For example, I love you buy, virus and was the total threat worldwide which was the cause of innovation of several new and more effective antivirus software e.g., Jaw, Quick Heal, Mobile Anti viruses, Main characteristics, of viruses are:

1. A virus is a self-replicating programmed whose main purpose is to propagate itself at as many different places as possible
2. A virus can any propagate itself by an unknown act of a user of the system in which it exists.
3. A virus propagates itself by modifying anthem programme to include itself.

It would be no exaggeration to say that there is a cyber-crime wave in recent year. Presently, viruses are the crime most common problems which the causing serious damage to computer system. Viruses are a program or code damage that replicates and infects another programmed, or sector or document by inserting itself or attaching itself to that medium. The effect of virus is that it destroys of attars the data files and other programmed.

Except in rare cases the virus the does not damage computer hardware. For instance, love bug virus of May, 2000 caused severe damage, to working internet sites. There are more the than 5000 different strains of viruses of across the global. So, also virus recently is developed by Pakistan has defaced the Indian website generally. There are two main classes of viruses. The file infectors, which attach themselves to ordinary programme files. File infectors of can either be direct action or resident.

A direct action virus select one or more of the other programmed to infect each time of programmed that contains it, is executed. A resident virus hides itself somewhere is memory. The first time on infected programmer's is executed, and there after infects other programmer when they are executed [5].

The second category of viruses is boot- record infector, these viruses executable code found in curtain system areas on a disk, which are not ordinary files. Examples include Brain, Stoned, Azusa, Michelangelo etc. which are always resident viruses. However, there are attain viruses which are able to infect both hence they are called "bolo and file" versus.

A versus hoax generally appears an e maim, message that Describe a particular virus that does not in fact exist such message are intended the create pane to computer users. The writers or writers email the warning and include a plea for the reader to for word it to other. The message then spreads like a chain letter. Propagating throughout the internet the individuals receive it and then innocently forward it.

For example, "good times" virus harks was written in 1994 and since then the carded the globe many times. It rather than acting upon it. Beside virus, there are some common cyber offence which are divested, against the computer systems, network, are or data while there are others in which computer is used as an instrument for community crime.

1.19 Violation of Privacy

Privacy is the claim of individual, group or institutions to determine for themselves when, how and to what extend information about them is communicated to other on not. In the District Registrar & Collector v. Canara Bank [6], states that privacy defined as "The state of being free from instruction of disturbance in one's private life or affairs.

In. R. Rajagopal v. State of Tamil Nadu [7]. The right of to privacy has been defined by justice lives, D. Brandies of The American Super could court as The eight to be let alone the most comprehensive of right and most valued, by

civilized men" In this case the court observed: "A citizen, has a right to safeguard the privacy of his own, his family marriage, procreation, motherhood, child, bearing and education among the other matters. None own publish anything cannoning the above matters without his consent-whether truth full or otherwise and whether laudatory or critical.

In Radha v. State of U.P [8] The Allahabad High Court, holding that prostitutes were also entitled to the might to life, directed the police to investigate or not to quiet them for their residence and not to brass them, except in accordance with law. The Government was also directed to provide them with some technical training as to enable them to earn their bread through the some of technical skill

Privacy in the technical driven world is a different proposition. Technology has become a kind of double-edged sword, on one hand it equips of the person to safeguard his privacy and on the other it helps in blowing the privacy cover, on many have had.

There are means to computer the digital footprints of the user who is browsing the internet for various personal reasons. It is a kind of personality identifiable information address. It is a kind of automatically computed by another computer when any communication link is made over the internet. The computer resource in use could be easily to be identified as it has been given a unique if address b the internet service provider. It is represented ted by four members that range from 0 to 225. Whenever a person browser, visit a sites, sends an e-mail or chats online, the leaves his distinctive'. In address behind It is possible, either by searching IP registration data bases or by conducting a trace route, to determine an approximate physical location of an IP address.

In case of unauthorized disclosure of information of any person without his consent in violation of privacy of said person which it is not a is public welfare then the person who disclose of information shall be punished with imprisonment for a term, which may extend to two years a with fine, which may extend to one lakh rupees or with both.

As highlighted in the aforesaid discussion the issues of right of privacy of as enumerates of act should be read along with eight reasonable restriction imposed by article 19(2) on "right to freed or expression of Article 21 right to life and person as liberty which states that one no person shall be deprived of his life or personal liberty except according to procedures established be low"

1.1.10 Email Fraud (Spamming)

E-mail is an inexpensive and popular device for distributing, fraudulent message to potential victims, This technical not only helps of to assume someone else' identity, but also helps to hide one's own. Therefore the person community the e-mail has little of being detached and identified. The most common e-mail fraud in phishing I.e., personal information fraud the purpose of such spasm is to trick the person for divulging his person information so that the offender can steal his identity and commit crime in that person's name.

Since electronic funds transfer system have now begun to proliferate there is greater risk of transactions being intercepted or diverted. Now is a day valid credit cards number can be intercepted electronically as well as physically and the digital information stored on a card can be counterfeited. Section if of the copyright act makes internet fraud as a offence. Punishable with imprisonment up to two years or with five fines which may be extend to rupees one lakh.

1.1.11 Cybercrime related to intellectual property

Intellectual property consists of a bundle of rights which many be violated by community software privacy, copyright infringement trade mark and service mark violations, there of computer source code etc. Internet being, the computer source fastest tale communications and information systems, it has become a most convenient media, to conduct business, transaction become a most action. The explosions of digitalization and the internet have further facilitated the intellectual property right violence to copy and illegally distribute trade secures, theft of computer source code etc. Computer private steal away valuable intellectual property when they copy software music, graphics picture books, movies etc. which are available on the internet.

Usually most material that the pirates or offenders want to copy is protected by the copyright which implies that a person can't take our copies thereof unless permitted to do so by the copyright owner. It punishable offence do under the copyright [9]. Right the various acts to which copyright Act, 1957 extends are enumerated in section 14 of the Act

Trade mark is also one of the intellectual property right to that the protect good will and reputation of traders and businessmen. These marks and are intended to differentiable of a goods of traders from other traders who are in the some strum of trade or business [10].

Passing off actions are also covered under the Trade mark Act wherein a trader passes of his inform quality goods in the name of some reputed traders who is selling the same commodity or article. Thus, if a particular, log is generally associate with and used in relation to product, A its use of by someone else is relation to product "b" would be an infringement of trademark right and an act of passing off than these illegal activities are curried on through the use of computer of Internet, It will be attract of the provision of the information of Technology Act 2000.

Thus in Ridiff Communication Ltd. v. Cyber both and Ramesh Nahata [11], The High Court of Bombay held that "a domain name is more than a interned address and therefore entitled to protection under the trademark Act, 1957".

M/S Sattyam Infoway Ltds v. M/S Sifynet Solutions (P.) Ltd [12].

In The Supreme Court ruled that with the increase of commercial activities on the internet, a domain name is also used as a business identifier. It is any serves as the address for internet a communities but also identifies the specific internet site for a specific business or its goods are services. It therefore, all the characteristics of a trademark and a passing off action can e based for infringement of domain name right.

The apex court hold that by adopting a sin line and deceptive name siffy which was phonetically similar to that of the appellant's they had the tried the cash internet services. Therefore the appellants were entitled. to relief.

It may be noted that just as the legitimate business organizations in the private or public sector rely upon information of system for communications or record defying, so also the cyber-criminal organization carry on that the illegal activities of using enhanced cyber space technology community on the respect. Eric erred one of the

official of the international chamber of commerce has predicted that information of technology of is not many of has reshaping of the made of corporate of functioning and energy of new business strategies but it is dramatically increasing the number of potential criminals.
According to him, there is bound to be cyber simultaneous increase in the influence of cybercrimes with new internet sites and uses which currently total around 40 million World Wide.

1.1.12 Email spoofing
A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator. A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates. For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

1.1.13 Computer Vandalism
Password or having created a new identity by fooling the computer into thinking has the system operator. Literally speaking, vandalism means destroying or damaging property of another. In the context of cybercrime, computer vandalism include within it any kind, person. It may be in the form of theft of a computer of some part thereby of peripheral destroy of the computer hardware, computer source of code, of the computer information, private source code, there computer information, private of the computer software are include in the computer vandalism. It computer vandalism is new type of cybercrime.

1.1.14 Money Laundering
It is a kind of cybercrime in which money is illegally downloaded in transit there is a phenomenal increase in the incidence of this cyber offence. Out of the 146 seizes made by the enforcement directorate in money laundering of cases of the year 2005 recoveries made in 106 cases involving seizure of about 9.5 of crores of rupees. Money laundering is crime which related the money of banking system. In the money laundering the money in transfer unauthorized way to own account in the theft of identity of person, his password and account number of this type of crime is increase in day and by day. This type of crime in increase in computer and other electronic devices and theft of hour's identity password, account number of to transfer the money to an account number of to another, this is new type of crime.

1.1.15. Data Diddling
This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy. This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is related on the scan. In this data are changed of computer system, record are destroy of and alterations of information of and other type of frauds. Data diddling of related to the new types of cybercrimes of because of in present of senior all information & documents of are prepare of through the electronic forms. Data diddling may be increased in day by day and new scan are present in every day.

1.1.16. Cyber Defamation
Defamation is defined is as an international false communication either published or publicly spoken, that injustice another's reputation or good name:. The gift of defamation is actual or presumed damage to reputation flowing from publication. In other words defamation flows, from publication or communities of making publicly known. Publication means that action of making internet the term publication includes dissemination, transmission and storage, of information or data in electronic form.
In India, issue of defamation has so for been dealt under the provision {Ss 499-502} of the Indian Penal code, 1860 the code make, no distinction between a slander and a libel. It define, defamation as "section 499: Whoever by words, either spoken or intended to be read, or by signs or by visible representation makes or publisher any imputation or knowing or having reason to harm, believe, that such imputation will harm, The imputation of such person, is said, except in the case hereinafter excepted to defame that person.
That defamation could also happen by means of signs of 'visible' representatives has included every pass possible form of defamation, including defamation in electronic form as well. Instance of defamation in receiving, ' defamatory' e-mail, online bulletin sending boards messages, chat room messages music downloads, audio files, seeming victors, digital photographs etc. on the internet. Even sending, defamatory, SMS, MMS, photographs and videos on mobile phones would etc be considered instances of defamation in electronic forms. In other words, the code is sufficient in itself to tackles any online defamation matter.
The publication has occurred, in what form of publication has happened? It is an important issue is technological or transmission, whether audio, video, mode of publication environment, whether a it looks into the mode of multimedia. Interest publishing in ann. electronic generating sending or receiving defamatory, email online bulletin board message, chat room, message, music downloads audio files, screaming videos, digital phonographs etc, on the internet.
Cyber defamation is not different from conventional defamation except that in involves the use of cyber space medium. Any derogatory statement or which the in intended to injure of person's name or reputation on a website, or sending email containing of defamatory of information's of some other person constitute the offence of cyber defamation.
Publication of a statement through the electronic mail, computer, dissemination, message chat room message without justification of excuse of reputation of which is collected in to injure of the another ending, to bring him into thinking members of the society estimate of right thinking example, charge of any criminal offence, or of fraud dishonesty immorality of dishonest conduct of etc. amounts of defamation.

1.1.17 Pedophilia
In internet despite its many benefits, has unfortunately provided pedophiles with a new tool. Offering ratite

anonymity for sophisticated uses and continuous access. The internet has made it easy for child pornography to distribute their materials and for pedophiles of to tube and prey on children. As a result, child pornography, it traded 24 hours as day in online chartrooms and in Internet Relay chat channels, and thousands of image of child sex abuse are available in easily accessible news groups, IN addition pedophiles can luck around, chat channels and rooms and message boards and use email to children for sex.

The prosecution of internet related child pornography and leaving cases in increasing. The department of justice has found that prosecution these cases has increased had found that prosecution by 10 percent every year since 1995 last year. The department of justice experts of have prosecuted over 400 such cases. Many of these cases our international investigation, between the customs, service and the English National crime, squall, involved over 100 members of a major pedophile ring that operated that in 21 countries. The internet and other forms of electronic communities and exciting opportunity of electronic communities offer new and exciting opportunities. For children they also expose children to new threats. For example federal law enforcement agencies have encountered numerous instance of in which adult pedophiles have which adult established relationship with child and later made contact for the purpose of engaging in criminal, sexual activities the purpose of engaging in criminal sexual many federal laws that have traditionally protected Children, such as those used to combat child pornography and leaving also apply when individual use the internet to commit those offense.

Other laws have specifically been designed to deal with online child pornography and related crimes- Federal agencies. Including customs service and the Department of Justice, have developed numerous programme to protect children on the interest. These have for the most part, been successful. Despite the successes. Law enforcement agencies still faced numerous challenge in combating online child pornography and related crimes. The most daunting of these challenges are the anonymous nature of the Internet and the need for extensive coordination and communication between federal, state and local law enforcement agencies.

The Department of justice, through the offline of juvenile justice and Delinquency prevention's missing and exploited children program, provides funding to state and local law enforcement agencies to create multijurisdictional, response of prevent and combat internet fictional response to prevent and combat crime against children.

There are steps parents and other can take to protect children from online dangers. Parents should be teach their children are follow the common sense. Rules of the road, for the Internet, including the need to protect of their privacy in the online world. Individuals of should be report inappropriate behavior of their Internal service provider or it is involves of the illegal of conduct, to agencies and need to establish and improve programmer that train their personal to recognize the seriousness of online child sexual exploitation and how to investigate this new form to criminal conduct.

1.1.18. Online Gambling

The growing availability of the internet of and other emerging technologies of had had to dramatic impale on gambling business of studies of estimate that bet 1997, and 1998. Internet gambling more than doubled from 6.9 million of the 14.5 million gambled. With revenues more than daubing from $300 internet $651 million a recent estimate reported 300 internet growth of internet of gambling of is alarming and has caused the several problems of for federal, state, tribal and local government in the enforcement of their gambling laws.

First: the internet is alternate to organized the crimes of groups of the that operate of gambling business to organized crimes of groups instantaneous and anonymous communication that can be difficult to trace to any particular individual, or organization there is no the possibility of abuse by unscrupulous gambling operations. The ability of for operator to alter, move or entirely removed sites from the internet written, minutes makes it possible for dishonest operators of to that take credit card numerous and money from deposited account and close down. Operators of may temper with gambling software to manipulate games to their benefit unlike the highly- jugulated physical word casinos, assessing the integrity of internet operation of in difficult gambling on the internet also may be provide on easy means for money laddering, as it provides criminal anonymity, remote access and access to encrypted data.

Second the anonymous nature of the internet also great the danger that access to internet gambling on their web sites. The government has received numerous complaints. From concerned and affected written regarding this problem.

Third, because the internet provides people with the opportunities to gamble at any time and from any place. Internet Gambling present a greater damage for compulsive gambler and may be cause server, financial consequence for the player and those dependent on the player resources As the National Gambling impact study commission, recently found.

Internet gambling is raising issue never previously addressed and exacerbating concerns associated with the traditional forms of gambling. While preventing underage grumbling and reducing problems associated with problems of gambling. The internet provides the highest level of anonymity for conducting gambling to date screening clients to determine age or its they have a history of gambling problems is difficult at best.

These problems are exacerbated the international scope of the interest. Although the United States has determined that there is a strong law enforcement priority of prohibit internet gambling other countries have a chosen to allow unrestricted betting and wagering on the interest. The United States Government in its assessment of existing and needed laws, must adopt solution foreign do not interfere that the operation of these lawful foreign gambling operations, while protecting its citizen from the transmission of bets or wagers into or from the countries.

Existing federal laws generally prohibit individual from transmitting bets or wagers on sporting events of contest in the us the advantage of the interest however, have made it necessary to update existing federal laws to ensure that they have are technology natural and prohibit new and well as traditional also needs better gambling activities. Law enforcement also needs better mechanism by which to track and identify online gambling business. The annoy nature of the interest complicates the ability of law enforcement to successfully track online gambling operators.

1.1.19. Sales of illegal Articles

Interest sales of illegal articles beverage have caused the direct shipments of such beverages of to consumers to

proliferate. Selling over the interest allows small illegal Articles producers to reach consumers well beyond their immediate areas. These Interest sales of illegal articles enable adults and potentials sinuous to receive products and that are not ordinary available through the traditional distribution channels.

Fifteen states have established reciprocal arrangements of that permit the shipment of illegal articles into their jurisdiction from one reciprocal state to another. Sales of illegal articles from one reciprocal state to another. Sales by illegal articles marketers are not however, limited to consumer in other reciprocal states to another. In money cases, these marketers may be sip to consumer in other states, a practice that may be violate state illegal articles control laws. Even if federal takes state paid on these products direct revenue and may consumer across state lines cause a loss of revenue and consumer are across state lines cause result in federal and state, regulatory violations. Such regulatory violence many include devilries to underage persons and the sale of unregistered articles in a state the sale of unregistered articles results in a loss of state registration fees, state excise for tax revenues and local sales for tax revenues.

The primary issues concerning the sales of illegal articles, over the internet the difficulty of sellers of have in determining whether a purchaser is underage. Some minors could whether a seek to use cards, legitimately or not, to conceivably seek a to use credit cards, to place on order through internet and have illegal articles delivered through a shipping company, several website requires purchasers to certify that they are of regal are either by clicking on part of the web page faxing a copy of lance. Restricting of the delivery of illegal article to situation where proof of age is obtained and recorded would assist in preventing access to illegal articles by underage persons. Currently however, there is a significant potential, for abuse in the sale of illegal articles to minors

A second investigatory issue related to the broader issue of jurisdiction. An out of state, seller that salver illegal articles, through a website is not generally loaned by the state, through the state courts, often have difficulty establishing as noted above ATF may take jurisdiction, and demonstrative action against a permitted that ships village articles into a state in violation of the laws that state this authority would not reach situations where a relation in one state, slips to a purchaser in another state, in because relations are not required result the illegal articles, But if the in state purchases relations then becomes a who sale agent, against whom ATF may take enforcement action. As existing laws address the legality of shipping and selling alcohols beverages in interstate commerce, the primary issue communing in the sale of illegal articles over the interest is the potential anonymity of the burger, The anonymous nature of the interest makes it, difficult, using current technology, for a seller to verity of at the time of sale whether a prospective purchases is a of legal sage of purchasing of articles of not. In addition of the interest facilities direct shipment of legal articles of prohibits of sales articles of consumer across state lines resulting in a loss of state of registration fees and state excuse and local sales the tax revenues and possibly resulting in federal or state regulatory violations

1.1.20 Page Jacking

Page- Jacking a new type of computer crime. Page Jacking involves the appropriation of web site description key words, of meta tare from other sites. The page jacked is sites, these items into his our sites, seeking to draw consumer to a particular site this is a because the descriptions, key words, and meta tag and used by search engines when sorting and displaying sits on a particular topic requested appear on individual. When the sites for a particular topic appear an individual might see two or three descriptions for what appear to be the same site. If the person happens for to click on one of the duplicated description or she will be directed to the flack site. When often in pornographic site. Complicating matters even further is that page- jackets often mouse trap of user browser of that attempt of to close the browser's windows of to use the back or forward button built of simply direct the user to another of pornographic site.

The FTC has taken the lead in addressing page-jacking In September 1999 the FTC announced that it had obtained temporary restraining orders on federal of district court against several web site of owner for page jacking. The FTC against several web site owner engaged in deceptive and unfair trade practices in violation of the FTC Act, Page Jacking could also potentially violence, federal intellectual portions of the imitated sites, than he might be criminally liable for copyright, trader mark, potent infringement. In a page jacked of into a domain name server and change the date to redirect visions of to the hackers site, that person could also be in violation of feral computer of crime statutes, sachems is 18 use 1030, which prefect the integrity of computer of systems of against hackers.

1.1.21 Online Securities Fraud

The interest has had a profound effect on how invest one resource and trade securities. Million of investors are signing on the interest to obtain investment information and to execute traders. Recent estimate are that close to 16 percent of all online traders are conducted crime online. The number of online a/c open of second quarter of 1999 nearly triple the number open as recently as 1997. The interest has brought significant benefits to investors, including changed to access information and lower costs to execute traders.

Unfortunately the interest also has opened new avenges for fraud artists to attempts to suitable the investing public. This is because the internet offers perpetrators of securities fraud a medium to commit their crime that is speedy cheap easy to use, and relatively anonymous. For the most part, there are three categories of frauds that have been encountered ogling by law enforcement.

Market manipulation fraud most often involves attempts to artificially inflate a stock of price of wearing the demand to for thinly of demand through the dissemination of false and misleading information, such as phony announcement pertaining to the strategic alliances, future learning, mergers, on or other importance corporate development. The internet has proven to the textile ground for the such manipulations, because information can be disseminated with simple click of mouse of millions of users via web site. Newsletters, span, message boards and other internet media. The manipulator normally ounces of shows in company's stock and sells during the run up that the manipulator water, This fraud commonly known as a pump and dump schemes. The

pair gain case discussed at the beginning of this report is an example of a market manipulation case.

Offering Frauds generally involve either false or misleading offerings and of securities. Falling into this category of cause are pylons and ponzi schemes and affinity frauds safeguard targeted out of specific social, ethics or religious without groups. In addition, there have been numerous frumenty offerings of non-traditional securities over the internet such as offerings or for prime bank program me and other esoteric securities including interests in frays, coconut plantations and fictional countries. Persons offering these securities often violate the law by failing to register as broker dealers.

Illegal touting securities frond takes place when persons are paid to tape of a company's stock without making legally required discloser of nature, source and amount the their compensation. This disclosure of in necessary because investors have a right to know whether information they are receiving is objective or bought and paid for.

The federal securities law provides textile but extensive mechanisms by which securities offenses can be procreated enforcement the substance still and may be adequate. Law enforcement agencies still and adequate resources to counter online securities fraud. As with other types of unlawful conduct on the internet the interstate and foreign nature of the internet hinders the ability of law enforcement of investigate and prosecute online criminals.

1.2 Mode and Manner of Committing Cyber Crime

2.2.1 Theft of information in electronic from

This in include Information stored in computer hard disks, removable storage media information etc. Theft may be either by appropriating the date physically by tampering them through the virtual medium

2.2.2 Salami Attacks

This kind of crime is normally prevalent in the financial institutions of or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration of so small that it would be normally go unnoticed.

2.2.3 Unauthorized access

This kind of offense is normally as hacking in the gentries sense The framers of the information of technology Act 2000 have used to of word, in hacking without changed unauthorized access as the letter had wide connotation.

2.2.4 Internet time thefts

Normally in these kind of theft the internet surfing housed is of the victim of are used up by another person. This is done of by giving access to the login ID and the Password.

2.2.5 Email Bombing

This kind of activity of rules of to sending large number of mail to the victim, which may be on individual or a company or even mail servers there by intimately resulting into crashing.

2.2.6 Logic Bombs

These are went dependent programmer. This is implied the at these programmer are weaned a to do something only when a certain event accuse. E. g Even some viruses may be termed Logic bomb because of they lie dormant all through the year and become they active only on a particular date.

2.2.7 Data Diddling

This kind of an attack involves patterning raw data just before a computer process of it and then changing it back after the processing is completed. The electricity board faced similar problem of data duding while the department was being computerized.

2.2.8 Do mail of service attack

The computer of the victim of flooded with more request of than it can handle which cause it to crash distributed denial of service attack is also a type of denial of service attack in which the offenders of wide of in number of and widespread.

2.2.9 Trojan attack

This term has its origin in the word; Trojan horse: In the software filed the means of on unauthorized programmer. Which the passively gains control over another's of systems by representing itself an authorities programmers.

2.3.10. Worms Attacks

Viruses are programmer that attack themselves to a computer or a life and then circulate themselves to other files and then circulate other computer on a network they usually affect the data on a computer, either by attiring of duding it.

2.2.11 Web Jacking

This term is derived from the term is jack ling. In the these kinds of offense of the hacker gain access and control over the website of another. This is may be done for fulfilling of political objectives for money. The web jack ling is a process where are control of over the site of another is made backer by some considerable of it.

In this chapter we have defined the various kind of cybercrime. Like Hackling, Defamation, Fraud Left stalking, Pornography, Paedophillia, Online Security, fraud Spanning, Email Spoofing, Intellectual property crime.

Money laundering, Data diddling, page- jacking various other kind of cybercrime. In this kind we knew that cybercrime is very dangerous to society it effect the social political and economic or security of system of the society. We adopt to preventive measure. To control of the various type of the cybercrimes.

References

1. Diwan Prag. Cybercrime & E-commerce law.
2. Parker Doon. Crime by computer.
3. S/66 Information Techology Act, 2000.
4. S/66 Information Technoiogy Act, 2000.
5. Jreusalem 185 virus is an example of resident file infectrvirus.
6. AIR. (1) SCC 2005, 496.
7. AIR. SC 1995, 264.
8. AIR. NOV. 2000, 19. (ALL).
9. S/2(M) Copyright Act, 1957.
10. S/2(1) (2) (b) Trademark Act, 1999.
11. AIR. BOM. 2000, 27.
12. AIR. SC. 2004, 3594.