Cyber torts are the latest and perhaps the most complicated problem in the cyber world. Cyber torts may be said to be those species, of which, genus is the conventional torts, and where either the computer is an object or subject of the conduct constituting tort...

Cyber Torts

Cyber torts are the latest and perhaps the most complicated problem in the cyber world. "Cyber torts may be said to be those species, of which, genus is the conventional torts, and where either the computer is an object or subject of the conduct constituting tort". "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber tort

A generalized definition of cyber tort may be " unlawful acts wherein the computer is either a tool or target or both". The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases-unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

· Birth Of Internet Litigation

The Internet, which began as the U.S. Defense Department's ARPANET, was designed to link computer networks to various radio and satellite networks.25 The first judicial opinion to mention the Internet was United States v. Morris.26 The defendant in Morris was a graduate student who had released an Internet worm that paralyzed thousands of university and military computers throughout the United States.27 In the same year, Robert Riggs was prosecuted for gaining unauthorized access to a Bell South computer and misappropriating proprietary information about the telephone company's 911 system. He subsequently published this confidential data in a hacker newsletter.

It was not until 1994 that any plaintiff prevailed in an Internet tort case. In a controversial decision, an anthropologist was denied tenure at the University of West Australia in Rindos v. Hardwick. A rival anthropologist, Hardwick, posted a statement supporting the university's decision and accusing Rindos of sexual deviance and of research detrimental to the aboriginal people of Australia.30 Although an Australian court assessed this first damages award in an Internet tort case, the vast majority of subsequent cyber torts have been litigated in America. During the past decade, American tort law is beginning to evolve to address online injuries such as Internet defamation, e-mail stalking, spamming, and trespassing on web sites.

· Distinction Between Conventional And Cyber Tort

There is apparently no distinction between cyber and conventional tort. However on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber tort, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber tort. The sine qua non for cyber tort is that there should be an involvement, at any stage, of the virtual cyber medium i,e. Cyber space.

· Reasons For Occurrence Of Cyber Tort:

Hart in his work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber tort. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space- The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much more easier.

2. Easy to access-The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3. Complexity of systems-The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. These lucanas can be taken advantage of and computer security systems can be penetrated into.

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

5. Loss of evidence- Loss of evidence is a very common & obvious problem as all the data are routinely destroyed as they are updated every next moment. Further collection of data outside the territorial extent also paralyses this system of investigation.

· Mode And Manner Of Committing Cyber Tort:

1. Unauthorized access to computer systems or networks/Hacking-This kind of offence is normally referred as hacking in the generic sense. However the framers of The Information Technology Act 2002 have no where used this term and also the term "unauthorised access" has a wider connotation than the term "hacking".

2. Theft of information contained in electronic form-This includes information stored in computer hard disks, removable storage media, magnetic disks, flash memory devices etc. Theft may be either by appropriating or rather misappropriating the data physically or by tampering them through the virtual medium.

3. Email bombing- This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

4. Data diddling- This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The Electricity Board faced similar problem of data diddling while the department was being computerised.

5. Salami attacks- This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. The Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

6. Denial of Service attack- The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

7. Virus/worm attacks- Viruses 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 usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988 which almost brought the development of Internet to a complete halt.

8. Logic bombs- These are event dependent programs. This implies that these programs are created to do something

only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

9. Trojan attacks- This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

10. Internet time thefts- Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa's Case- the Internet hours were used up by any other person. This was perhaps one of the first reported cases related to cyber crime in India. However this case made the police infamous as to their lack of understanding of the nature of cyber tort.

11. Web jacking-This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently in the Case of MIT (Ministry of Information Technology) its site was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the 'Gold Fish Case'. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded as ransom. Thus web jacking is a process where by control over the site of another is made backed by some consideration for it.

· Who Are Generally Cyber Criminals:

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals-

1. *Children and adolescents between the age group of 6–18 years* –The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

2. *Organized hackers*-These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. Recently the Indian Government had been targeted with the same. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

3. *Professional hackers/crackers* – Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes. state databases and news services,41 (3) cyberspace research libraries of law firms,42 (4) national, regional, and local verdict reporters,43 (5) reports of domain name disputes,44 (6) individual cyberspace cases reported on law firm web sites,45 (7) law school research centers,46 (8) American Law Reports ("ALR") annotations,47 (9) all Internet-related Mealey publications,48 (10) e-commerce law secondary sources,49
(11) Internet

· A Broad Classification Of Cyber Tort.:

1. *Harassment via e-mails*- Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Recently I had received a mail from a lady wherein she complained about the same. Her former boy friend was

sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is a very common type of harassment via e-mails.

2. *Cyber-stalking*- The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

3. *Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) / Polluting through indecent exposure*- Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials. Downloading through the Internet, obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

4. *Defamation:*- It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. E.g. the mail account of Rohit was hacked and some mails were sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.

5. *Unauthorized control/access over computer system:*-This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

6. *E mail spoofing*- A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. Recently spoofed mails were sent on the name of Mr. Na.Vijayashankar (naavi.org), which contained virus. Rajesh Manyar, a graduate student at Purdue University in Indiana, was arrested for threatening to detonate a nuclear device in the college campus. The alleged e- mail was sent from the account of another student to the vice president for student services. However the mail was traced to be sent from the account of Rajesh Manyar.

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

8. *Intellectual Property crimes / Distribution of pirated software:*- Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc. The Hyderabad Court has in a land mark judgement has convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software.

9. *Cyber terrorism against the government organization:*-At this juncture a necessity may be felt that what is the need to distinguish between cyber terrorism and cyber torts. Both are dangerous acts. However there is a compelling need to distinguish between both these acts. A cyber tort is generally a domestic issue, which may have international consequences, however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks,

etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of – Osama Bin Laden, the LTTE, attack on America's army deployment system during Iraq war. Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives" Another definition may be attempted to cover within its ambit every act of cyber terrorism. A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to –

(1) putting the public or any section of the public in fear; or

(2) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

(3) coercing or overawing the government established by law; or

(4) endangering the sovereignty and integrity of the nation and a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

9. *Trafficking:-* Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.

10. *Fraud & Cheating:-* Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. Recently the Court of Metropolitan Magistrate Delhi (17) found guilty a 24-year-old engineer working in a call centre, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony website. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating under IPC but did not send him to jail Instead, Azim was asked to furnish a personal bond of Rs 20,000, and was released on a year's probation.

· Distinction Between Cyber Crime And Cyber Tort

There is specific distinction between cyber crime and cyber torts which has to be cleared when we are discussing cyber torts.

The cyber crime includes hacking/cracking, Possession of unauthorised information , cyber terrorism against government organisations ,distribution of pirated software , harassment through emails , cyber stalking , dissemination of obscene material on the internet , defamation , hacking/cracking , indecent exposure , computer vandalism, transmitting virus , internet intrusion , unauthorised control over computer systems , pornography , exposing the youth to indecent material , Trafficking. Cyber torts include cyber stalking , breach of privacy , cyber obscenity and cyber defamation. So there may be some elements which may be common in both but there are several differences between the two.

· Statutory Provisions:

The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which The Information Technology Act 2000 was passed and enforced on 17th May 2000.the preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, The Indian Evidence Act 1872, The Banker's Book Evidence Act1891 and The Reserve Bank of India Act 1934. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000. So that they may regulate and control the affairs of the cyber world in an effective manner.

The important sections are Ss. 43,65,66,67. Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Crore by way of remedy. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may

extend up to 2 years or both. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.

Adjudication of a Cyber Torts

On the directions of the Bombay High Court the Central Government has by a notification dated 25.03.03 has decided that the Secretary to the Information Technology Department in each state by designation would be appointed as the AO for each state.

Liability of intermediaries and the author under Indian law

The Internet has made it easier than ever before to spread a huge amount and variety of information worldwide. As mentioned earlier, SNWs are, at a grass root level, a medium for exchanging information between people. SNWs allow any person to write any statement, including the defamatory one, on their own or a third person's virtual profile. In this scenario, the question which naturally arises is: who can be sued by the person against whom such defamatory statement has been made.

Under the operative Indian law, the person who made such statement as well as its distributor and publishers can be sued. Apart from the author of such statement, intermediaries such as the concerned SNW, the website holder, the internet service providers, as well as the other users of such SNW on whose profiles defamatory statements have been written by the author, can be sued in their capacity as a publisher of defamatory statements and can be held liable for such statements. It is to be noted that such intermediaries or other users of SNWs may not be aware of such defamatory statements by the author on their own virtual profile.

Section 79 of the Information Technology Act, 2000

(the "Act") gives immunity to network service providers. According to Section 79 of the Act, a 'network service provider' (defined as a person who on behalf of another person receives, stores or transmits the electronic messages) shall not be liable under the Act, or Rules or Regulations made there under, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

The Information Technology Amendment Act, 2008

The Information Technology Amendment Act, 2008 was passed by the Indian Parliament on December 22, 2008 and following Presidential assent it has become a law from February 5, 2009. The amendment bears a certain degree of similarity to the prevailing law in the United States of America ("USA"). In USA, intermediaries such as SNWs, internet service providers and other interactive web service providers are exempted from liability under defamation if (i) they prove that they have no control over the statement or content and (ii) they remove such statement or content from their website or network immediately upon receiving the notice from the plaintiff.

The amended Section 79 of this Amendment Act provides the mechanism equivalent to the law of USA. Following are the relevant provisions of the Information Technology Act (after the said amendment comes into force).

Section 79:

(1) Notwithstanding anything contained in any other law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

(4) Intermediary shall observe such other guidelines as the Central Government may prescribe in this behalf.

Explanation.--For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary. Section 2(w) – "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes, but does not include body corporate referred to in section 43A."

· Analysis Of The Statutory Provisions:

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

1. The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

2. *"Cyberlaws, in their very preamble and aim, state that they are targeted at aiding e- commerce, and are not meant to regulate cyber torts" :-* Mr. Pavan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the I.T.Act 2000 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime. At this juncyure it would not be completely wrong to contend that the above statement by Mr. Duggal is not fundamentally correct. The reason being that the preamble does state that the Act aims at legalising e-commerce. However it does not stop here. It further amends the I.P.C., Evidence Act, Banker's Book Evidence and RBI Act also. The Act also aims to deal with all matters connected therewith or incidental thereto. It is a cardinal rule of interpretation that "text should be read as a whole to gather the meaning". It seems that the above statement has been made in total disregard of this rule of interpretation. The preamble, if read as a whole, makes it very clear that the Act equally aims at legalising e-commerce and to curb any offences arising there from.

3. *Cyber torts:-* The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T.Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber torts will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T.Act 2000 read with the Penal Code is capable of dealing with these

felonies.

4. *Cyber crime in the Act is neither comprehensive nor exhaustive:-* Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- "The IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime". Mr. Duggal has further commented, "India, as a nation, has to cope with an urgent need to regulate and punish those committing cyber torts, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes.

5.*Ambiguity in the definitions-* The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The infamous go2nextjob has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the netizens are till s. 66 exists in its present form. Further section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by the **Bal Bharati case.**

6. *Uniform law:-* Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber torts. Cyber torts are a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

7. *Lack of awareness-* One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling Microsoft pirated software over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for online cheating by buying Sony products using a stolen credit card.

8. *Jurisdiction issues:-* Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 is very silent on these issues.

9. *Extra territorial application:-* Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

10. *Raising a cyber army:-* By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI)) is definitely a welcome step in this direction. There are man cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –

Case 1: When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

Status: Probe on

Case 2: CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in
his bank account in Delhi.

Status: Chargesheet not filed

Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

Status: Pak not cooperating.

11. *Cyber savvy bench:-* Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. Mr T.K.Vishwanathan, member secretary, Law Commission , has highlighted the requirements for introducing e- courts in India. In his article published in The Hindu he has stated "if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System".

12. *Dynamic form of cyber crime:-* Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind." The (de)creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

13. *Hesitation to report offences:-* As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the Delhi time theft case. "The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business."This attitude of the administration is also revelled by incident that took place at Merrut and Belgam. (for the facts of these incidents refer to naavi.com). For complete realisation of the provisions of this Act a cooperative police force is require.

· Conclusion:

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime or either cyber torts from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to keep a check. Undoubtedly the Act is a historical step in the cyber world.We would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive and at the same time a vigil check should be kept on its misappropriation and further consequences.

****

Bibliography

• ***Books Referred***

(1) Cyber Crime And Corporate Liability-Wolters Kluwer-Rohas Nagpal
(2) Handbook Of Cyber Laws-Macmillan-Vakul Sharma
(3) Cybercrimes And Law (An Overview)-C.Vidya
(4) Ramaswamy Iyer-The Law Of Torts-A Lakshminath And M Sridhar

(5) Legal Era-II
(6) Nagpal R. – What is Cyber Crime?
(7) Sify News 14.03.03
(8) Deccan Herald 16.03.03
(9) Hindustan Times 03.03.03
(10) Nagpal R- Defining Cyber Terrorism

• Websites Referred

(1) http://www-bcf.usc.edu/~idjlaw/PDF/13-1/13-1 RustadKoenig.pdf
(2) http://www.ebooksdownloadfree.com/Security/Cyber-Situational-Awareness-Issues-and- Research-BI10250.html
(3) en.wikipedia.org/wiki/Cyber law
(4) http://www.cyberessays.com/lists/cyber-torts/page0.html
(5) http://www.slideworld.com/slideshows.aspx/CHAPTER-4-Torts-and-Cyber-Torts- ppt-2225880