IMPORTANT CYBER CRIMES AS A CONSEQUENCE OF TECHNOLOGY

BY

MISS ASHWINI DOMINICA COLAÇO

SYLLM

G. R. KARE COLLEGE OF LAW, MARAGO – GOA

INDEX

OBJECTIVES

The main objective of this research is:

1) To critical analyzing the nature and causes of Cyber Crimes

2) To find out the problems of jurisdiction of Cyber Crimes.

3) To find out and analyze the laws and other problems of prosecution and investigation of Cyber Crimes in India.

4) To find out the problems in relation to enforcement and judicial problems.

5) To analyze the reasons for failure of legal mechanism to curb the growing instances of Cyber Crimes.

6) To suggest the appropriate changes of laws in relation to Cyber Crimes.

7) To suggest the appropriate changes in the constitution and modus operandi of investigation and prosecution mechanisms.

INTRODUCTION

With the era of modernization and growth in India and all over the world, use of internet has also grown rapidly. With the rapid increase in the use of internet, there is also an increase in illegal activities and crime that is committed through internet. No doubt with the advent of internet facility work has become a lot easier and efficient in every field be it entertainment, business, sports, academics, or any other field, but just as every coin has two sides to it internet or cyber technology has its own advantage and disadvantage, disadvantage in the form of illegal activities commonly known as "*cyber crime*".

Cyber crime has no specific definition. It is nowhere defined in any act or statute. It is quite similar to conventional crime both consist of act and omission and breach of law which has been set up by the state. According to Cambridge dictionaries cyber crime is defined as a "*criminal or illegal activity that is done using internet*". This crime ranges from committing fraud to child trafficking through pornography which further goes up to stealing identities and interfering with their privacy. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. Cyber crime may be said to be a genus is the conventional crime, where either the computer is a tool or medium of conducting or committing crime. This growing danger from computer crimes has now awakened most of the states to protect its citizens against such harm. New laws have been formulated to raise the voice against cyber crime but what is needed is proper implementation and enforcement of these rules. [1]

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 concept to the new emerging crime of cyber law it can be rightfully said that to protect against this crime also an efficient and effective rule of law is needed.[2]

The computer crimes can be broadly divided into two groups – computer crimes where the accused is a computer, victim is a computer and the tool used to commit the crime is also a computer. The second group is the computer related crimes. Here the computer becomes a part of the evidence and a crime has taken place with the help of a computer or where the computer forms a part of the complete crime scene. To deal with these two broadly divided groups we have laws in India that take care of them, once they fall in their purview. For the first group, the Information Technology Act, 2000 has been evolved whereas the second group attracts the provisions of IPC, Cr.PC, Indian Evidence Act, and Law relating to Intellectual Property Rights, etc.[3]

Before the advent of computer crimes, the law enforcement agencies were bound by some ground rules. There established procedures, for investigation and prosecution of all types of crimes, large number of physical evidence is generally available at the scene of crime.

[1] http://www.crimeresearch.org/analytics/702/
[2] Ibid
[3] Barkha & U. Rama Mohan, Cyber Law & Crimes – IT Act 2000 & Computer Crime Analysis, New Ed. 2006, S. P. Gogia (H. U. F.) Publications, p. 1.

Collection of such physical evidence materials needs a lot of common sense and a little technical knowledge. Information technology provided an opportunity to the criminal to commit traditional crimes like cheating, fraud, theft, embezzlement of bank deposits, credit card fraud, industrial and political espionage etc. at the same time, it helps in perpetrating non-traditional information technology specific attacks, against the security of critical infrastructures like telecommunication, banking or emergency services. Various surveys indicate that the attacks on the computer systems are going to increase manifold through telecommunication networks, theft of telecommunication services and the use of computers to commit crimes of data manipulation.

The society is moving from paper based to paperless scenario, from centralization, from controlled access to totally independent access and does on. In such a scenario, it becomes possible for the anti-social elements to cause havoc with minimum retribution from the existing criminal justice system. Traditional methods of crime detection, evidence collection and prosecution have become ineffective in combating the new challenges posed by perpetrators of computer crimes.

In this era of fastest information exchange though e-commerce, international trades and booming international trades and sharing of knowledge through this medium of communication are positive effects of internet, on the other side the internet have become one of the mediums of commission of crimes. There are various offences that could be easily committed through the abuse of this medium and there are well known impediments and hurdles that come in the way of prosecuting the offenders and enforcement of judgments of courts. The peculiarity of this medium of commuting offence has brought about various problems for laws enforcement authorities. The problems which generally arise in the way of enforcement agencies could be divided under the following heads:

1) Problems of Jurisdiction:

The first and foremost pr problem which arises in the enforcement and prosecution of cyber laws is the problem of jurisdiction. As we all know that different jurisdictions of world have their own fully fledged systems of prosecution and enforcement of criminal laws but they lack in legislating laws in regard to cyber laws and cyber terrorism which could be enforced without any impediment in any jurisdiction. The problem of reciprocity and reciprocal arrangements between nations is a part and partial of the problem of jurisdiction. A cyber criminal can commit a crime sitting at one jurisdiction whose impact or under come may ensue in the other jurisdiction or jurisdictions. The most prevalent crimes of this nature are crimes related to financial frauds, cyber terrorism, cyber stalking, pornography, etc. and when a crime ensues in any particular country or jurisdiction the authorities face the problem of jurisdiction because an act may or may not be a an offence wherefrom it has been committed. And the second most prominent problem that arises in regard to jurisdiction is that a country may not support the other country due to bad diplomatic relations and may raised the technical objections in regard to jurisdiction.

2. Problems with Investigation and Prosecution:

The investigation and prosecution of cyber offences is the second problem and impediment the comes in the way to curb cyber offences. India has old system of courts and prosecution mechanism. Absence of proper legislations and lack of knowledge of judges and prosecuting agencies in specific instances of cyber crime are the hurdles that normally come in the way investigation and prosecution. Investigation under the Indian system is generally done by police authorities who are not so aware about the developments and modes which are opted by cyber criminals. Lack of their knowledge about computers and modus operandi of criminals active in the cyber space is beyond even from their imagination. They are expert and habituated of investigating the traditional offences. The problems that generally arise in investigation and prosecution of cyber crime may be summarized as following:

a) Lack of proper legislation for investigating and prosecuting cyber offenders.

b) Lack of knowledge of police officers investigating those offences.

c) Burden of cases on the courts.

d) Delay in deciding cases under the present system.

e) Insufficient punishment (penalty, and imprisonment).

3. Problems of Enforcement:

The third impediment that comes in the way of curbing the menace of cyber crimes is the problem of enforcement. When an offence is committed in one jurisdiction and the offender is physically present and is subject of that particular jurisdiction no such problem arises because the territorial jurisdiction, laws applied and the prosecution and investigation mechanism belong to one single system but in offences related to cyber space the crime may be committed from altogether different jurisdiction where there may be difference of law and prosecution system and investigation mechanism so, a problem in regard to enforcement arises in such cases. That country may not ready to extend to offenders or may not ready to punishment.

4. Problems of Conflict of Laws:

Conflict of law may be in the generic sense be referred as the difference between laws pertaining to different jurisdiction related with same or similar set of facts constituting an offence. When we talk about criminal offences and conflict of law in that regard may be referred as the difference in quantum of punishments, imprisonment, definitions in the laws, etc. Every country is a sovereign state and capable of legislating on any subject according to the diverse cultural, social, economic, and other needs. So, a difference of legislation is always there between laws of different nations because the cultural, social, economic and even the moral scenarios are different in different countries.

5. Problems of State Sovereignty and Non-Cooperation between Nations:

One of the most prevalent problems which arise in the prosecution and investigation of offences pertaining to cyber space is non cooperation between the nations. The bad diplomatic relations could be one of the most prominent reasons for raising the technical objections of jurisdiction to harbour the offenders of enemy nation. If the nations cooperate well among themselves and make necessary reciprocal arrange arrangements among themselves for prosecution and punishment of offenders the instances of these offences may lessen to a great extent. Often the long administrative formalities, lack of extradition arrangements and lack of cooperation by a country where in the offenders take harbour result in evasion of offenders from law and they are often encouraged to repeat the occurrences of crimes.[4]

[4] www.directionsmerg.com

SCOPE AND KINDS OF CYBER CRIME

Various types of cyber crime are prevalent in the country. The computer cr4imesa enlisted have been classified into the following categories:

(a) CONVENTIONAL CRIMES THROUGH COMPUTER:

Cyber defamation, digital forgery, cyber pornography, cyber stalking/harassment, internet fraud, financial crimes, online gambling, and sale of illegal articles.[5]

1. Cyber Defamation:

The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public. Cyber defamation is a new concept but the traditional definition of the term defamation is application to the cyber defamation as it involves defamation of a person through a new and a virtual medium.

Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation. The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world. Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published.

The following are mediums by which offense of cyber defamation can be committed:

1) World Wide Web
2) Discussion groups
3) Intranets
4) Mailing lists and bulletin boards
5) E-mail

There are two broad category of case falling under cyber defamation:

1) The first category involves the cases in which the liability is of the primary publishers of the defamatory material, e.g. web site content providers, e-mail authors etc;

[5] Edited by S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, ed. 2004, Published by Prof. (Ms.) S. K. Verma, Director, for Indian Law Institute, Bhagwandas Rd, New Delhi, and Printed at Shivam Offset Press, New D3elhi. p. 233.

2) The second category involves the cases involving the liability of the internet service providers or bulletin board operators.[6]

2. Digital Forgery:

In a cryptographic digital signature or MAC system, digital signature forgery is the ability to create a pair consisting of a message m and a signature (or MAC) σ that is valid for m, where m has not been signed in the past by the legitimate signer. There are three types of forgery: existential, selective, and universal.

a) Existential Forgery: Existential forgery is the creation (by an adversary) of at least one message/signature pair (m, σ), where σ was not produced by the legitimate signer. The adversary need not have any control over m; m need not have any particular meaning; and indeed it may even be gibberish — as long as the pair (m, σ) is valid, the adversary has succeeded in constructing an existential forgery. Existential forgery is essentially the weakest adversarial goal, therefore the strongest schemes are those that are "existentially unforgeable".

b) Selective Forgery: Selective forgery is the creation (by an adversary) of a message/signature pair (m, σ) where m has been *chosen* by the adversary prior to the attack. m may be chosen to have interesting mathematical properties with respect to the signature algorithm; however, in selective forgery, m must be fixed before the start of the attack. The ability to successfully conduct a selective forgery attack implies the ability to successfully conduct an existential forgery attack.

c) Universal Forgery: Universal forgery is the creation (by an adversary) of a valid signature σ for *any* given message m. An adversary capable of universal forgery is able to sign messages he chose himself (as in selective forgery), messages chosen at random, or even specific messages provided by an opponent.[7]

3. Cyber Pornography:

One of the most heinous crimes committed through internet is use and abuse children sexually, worldwide. The use of internet now is growing day by day. Internet, now, at a very fast rate becoming a household commodity in India. Its maximum use nowadays has made the children a viable victim to the cyber crime. As more homes have access to internet, more children are using the internet and more are the chances of falling victim into such illegal traps. The pornographic content is easily accessible to the children. The easily accessible material have made children are more prone to such crimes. Sometimes Paedophiles contact children in the chat rooms posing as teenagers or a child of similar age; they start becoming friendly with them and win their confidence. Then slowly paedophiles start sexual chat to

[6] http://www.helplinelaw.com/docs/main.php3?id=CDII2
[7] http://en.wikipedia.org/wiki/Digital_signature_forgery

help children shed their inhibitions about sex and then call them out for personal interaction. Then starts the actual exploitation of the children, By offering them some money or falsely promising them good opportunities in life, they force the child to indulge in bad activities, resulting in their exploitation. The paedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet. In physical world, parents know the face of dangers and they know how to avoid & face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways.

Most of the children and parents are unaware of internet knowledge. Thus, since they don't have proper guidance they become more lure towards criminal activities.

There is no exact or particular definition of obscenity. There is possibility that simply sexually explicit content is obscene in one country but it may not be considered as obscene in another country. Pornography on the Internet is available in different formats. It is difficult to limit the availability of pornographic content on the Internet. There are pictures, videos, animated movies; sound files etc are easily available on internet. People use internet to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive.

In India the **Information Technology Act, 2000** covers cyber pornography. According to section 67 of the IT Act "*Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.*"[8]

4. Cyber Stalking/ Harassment:

Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. The definition of "harassment" must meet the criterion that a reasonable person, in possession of the same information, would regard it as sufficient to cause another reasonable person distress. Cyber stalking is different from spatial or offline stalking in that it occurs through the use of electronic communications technology such as the internet. However, it sometimes leads to it, or is accompanied by it. Both are

[8] http://cyberlawpioneers.com/index.php/cyber-pornography/

criminal offenses. Cyber stalking shares important characteristics with offline stalking; many stalkers – online or off – are motivated by a desire to control their victims.

A cyber stalker may be an online stranger or a person whom the target knows. A cyber stalker may be anonymous and may solicit involvement of other people online who do not even know the target. Cyber stalking is a criminal offense that comes into play under state anti-stalking laws, slander laws, and harassment laws. A cyber stalking conviction can result in a restraining order, probation, or even criminal penalties against the assailant, including jail.

Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. These small acts may be followed by serious violent acts such as physical harm to the victim. Mainly the stalkers are male and those who are trapped of such activities are females, but sometimes it's other way round also. Most of the stalkers who engage themselves in such activities are dejected lovers or ex-lovers, who failed to satisfy their sexual urges, are harassing other victims to fulfil their desire.[9]

5. Internet Fraud:

The use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them, for example by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Internet fraud can occur in chat rooms, email, message boards, or on websites. Some more examples are - purchase frauds, counterfeit postal money orders, cash the cheque system, re-shippers, etc.[10]

6. Financial Crimes:

Financial crimes are crimes against property, involving the unlawful conversion of the ownership of property (belonging to one person) to one's own personal use and benefit. Financial crimes may involve fraud (cheque fraud, credit card fraud, mortgage fraud, medical fraud, corporate fraud, securities fraud (including insider trading), bank fraud, payment (point of sale) fraud, health care fraud); theft; scams or confidence tricks; tax evasion; bribery; embezzlement; identity theft; money laundering; and forgery and counterfeiting, including the production of Counterfeit money and consumer goods.

Financial crimes may involve additional criminal acts, such as computer crime, elder abuse, burglary, armed robbery, and even violent crime such as robbery or murder. Financial crimes

[9] http://en.wikipedia.org/wiki/Cyberstalking
[10] http://en.wikipedia.org/wiki/Internet_fraud

may be carried out by individuals, corporations, or by organized crime groups. Victims may include individuals, corporations, governments, and entire economies.[11]

7. Online Gambling:

Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet. The Internet has made way for new types of gambling to form online. The recent improvements in technology have once again changed betting habits just as Video Lottery Terminal, keno and Scratchcards changed the gambling industry in the early 20th century. Internet gambling has become one of the most popular and lucrative business present on the Internet. In 2007 the gambling commission stated that the gambling industry achieved a turnover of over £84 billion according to the UK Gambling Commission. This is partly due to the wide range of gambling options that are available to facilitate many different types of people.[12]

Gambling in India is heavily restricted but the opposite is true online. Approximately 40% of internet users in India have admitted to visiting a gambling site - but not placing a bet. The sites were primarily for lottery, cricket and horse betting fixes. The Public Gambling Act of 1867 prohibits running or being in charge of a public gaming house. The penalty for breaking this law is a fine of ₹200 or imprisonment of up to 3 months. Additionally, this Act prohibits visiting gambling houses. A fine of ₹100 or imprisonment of up to one month is the penalty. The Information Technology Act 2000 regulates cyber activities in India and prohibits publication or transmission of information that can corrupt people. This includes online gambling and the punishment for such activities is much more serious than for offline gambling operations – the fine is ₹100,000 or imprisonment up to 5 years.

Despite the existing prohibitive legislation, there is extensive illegal gambling throughout the country. The Indian gambling market is estimated to be worth US$60 billion per year, of which about half is illegally bet. According to the Indian National Newspaper, the Chief Executive officer for the International Cricket Council (ICC) said he was in favour of legalizing sports betting. He believes the illegal funds profited are through underground bookies that used the money to fund terrorism and drugs.

Only two states allow casinos, Goa and Sikkim. There is one casino in Sikkim and 12 in Goa, of which seven are land based and five are floating casinos that operate on the Mandovi River.

Other than lotteries, legal gambling in India is limited to betting on horse racing.

Online gambling is in its infancy in India, but Sikkim planned to offer three online gambling licences in 2010. This failed despite India being the most sought out country for online gambling. Sikkim also permits an online lottery, operated by Play-win, which takes bets from players throughout India. It is expected that other states will follow Sikkim shortly, thereby opening up a major online gambling market throughout India.

[11] http://en.wikipedia.org/wiki/Financial_crimes
[12] http://en.wikipedia.org/wiki/Online_gambling

In May 2011 India passed the Federal Information Technology Act which tries to put a stranglehold on internet gambling. This new act, which covers gambling sites, holds the Internet Service Providers responsible for blocking offshore betting sites.

One of the biggest obstacles faced by sports bettors in India is the fact that depositing to foreign bookies is extremely difficult. Typically, the majority of users deposit to online bookies using Money bookers or Neteller. Some attempts to deposit using a Visa or MasterCard may fail. The same is true of online bank transfers. In order to circumvent these blocks, savvy internet users have started to use Ewallet services for depositing. These services add a middle layer to disguise the nature of transactions, enabling users to get around the blocks by first depositing to a Ewallet and then using that Ewallet to fund an online betting account in Rupees. This is important because it circumvents legal issues that may have arisen about Foreign Exchange law.[13]

8. Sale of Illegal Articles:

It is becoming increasingly common to find cases where sale of illegal articles such as narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc. It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button.

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims. Many sites focus on selling prescription drugs and are referred to by some as "Internet pharmacies." These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the health and safety of patients. The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

As pointed out earlier, the online lottery is the most popular form of internet gambling in India. Most companies marketing and distributing or conducting state government-sponsored lotteries through the internet are not allowed to sell their services in the states that banned lotteries. In most cases, these marketers and distributors limit their online services to consumers who are residents of the states where a lottery is permissible. Notwithstanding the fact there has been no reported case of breach by any company promoting online lotteries, most of these companies (as a safeguard) seek an undertaking from their consumers relating to their residence. [14]

(b) CRIMES COMMITTED ON COMPUTER NETWORK:

[13] http://en.wikipedia.org/wiki/Gambling_in_India

[14]http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

Hacking/ unauthorized access, denial of service.[15]

1. Hacking:

Hacking in layman terms means an illegal intrusion into a computer system. Whatever act that is committed towards intruding into a computer network is hacking. Hackers with the help of programmers and readymade computer programs attack the computer to hack it. They possess the desire to perform such act and omissions; they even have an intention to do such illegal act. Some hackers are professional; they have made hacking their professional business but there are others who hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

Their main target is mainly extorting money from big corporate investors and government websites.

In the computer security context, a *hacker* is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word hacker exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the long standing hacker definition controversy about the true meaning of the term hacker. In this controversy, the term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a *cracker*, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.[16]

2. Denial of Service Attack:

The computer of the victim is flooded with more requests than it can handle which causes it to crash. Victims network or email box is flooded with spam mails which results in deprivation of the services which he is entitled to. Ultimately, this criminal act leads to denial of service attack. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Denial-of-service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo and eBay. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Sometimes, many computers are

[15]Edited by S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, ed. 2004, Published by Prof. (Ms.) S. K. Verma, Director, for Indian Law Institute, Bhagwandas Rd, New Delhi, and Printed at Shivam Offset Press, New D3elhi. p. 233.
[16] http://en.wikipedia.org/wiki/Hacker_%28computer_security%29

entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer.[17]

(c) CRIMES RELATING DATA ALTERATION/ DESTRUCTION:

Virus/worms/Trojan Horses/ logic bomb, theft of internet hours, data diddling, salami attacks, steganography.[18]

1. Virus Dissemination:

These are the malicious software, like Trojan horse, Time bomb, Logic Bomb, Rabbit virus, worms and Bacterium that attaches itself to other software. Viruses are type of programs that attaches themselves to a computer or a file and then act as a termite eroding other files on the computer and other computers on a network, thus, affecting the data on computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They make functional copies of themselves and continue with this process until they eat up all the available space on a computer's memory. E.g. *love bug virus*, which affected at least 5 % of world's computer. One of the examples of most degrading virus is the *Internet worm*, which caused lot of malicious erosions in the world computers.[19]

2. Theft of Internet Hours:

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. Illustration In May 2000, the Delhi police arrested an engineer who had misused the login name and password of a customer whose Internet connection he had set up.

The case was filed under the Indian Penal Code and the Indian Telegraph Act.[20]

3. Data Diddling:

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.[21]

One of the most common forms of computer crime is data diddling -illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school

[17]http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

[18]Edited by S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, ed. 2004, Published by Prof. (Ms.) S. K. Verma, Director, for Indian Law Institute, Bhagwandas Rd, New Delhi, and Printed at Shivam Offset Press, New D3elhi. p. 233.

[19] http://ahmedccna.blogspot.in/2012/03/virus-dissemination.html

[20]http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

[21] http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml

transcripts and virtually all other forms of data processing known. Section 66 and 43(d) of the IT. Act covers the offence of data diddling.[22]

4. Salami Attacks:

These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month. The attack is called "salami attack" as it is analogous to slicing the data thinly, like salami.

Illustration: Four executives of a rental-car franchise in Florida USA defrauded at least 47,000 customers using a salami technique. They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $1 5 per customer -difficult for the victims to detect.[23]

5. Steganography:

Steganography is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. The word *steganography* is of Greek origin and means "concealed writing." It combines the Greek words *steganos*, meaning "covered or protected," and *graphei* meaning "writing." The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other *cover text.* For example, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

[22] http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt
[23] Ibid

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.[24] This technology is now highly misused by terrorists in communicating with one another in carrying out terrorist activities and missions.

(D) CRIMES RELATING TO ELECTRONIC MAIL:

Spamming/ bombing, spoofing.[25]

1. Spamming/ Bombing:

Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, social spam, television advertising and file sharing spam. It is named for Spam, a luncheon meat, by way of a Monty Python sketch in which Spam is included in almost every dish.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions. A person who creates electronic spam is called a *spammer*.[26]

2. Spoofing:

In computing, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. The word "spoof" means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers tricking or deceiving computer systems

[24] en.wikipedia.org/wiki/Steganography#Use_by_terrorists
[25] Edited by S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, ed. 2004, Published by Prof. (Ms.) S. K. Verma, Director, for Indian Law Institute, Bhagwandas Rd, New Delhi, and Printed at Shivam Offset Press, New D3elhi. p. 233.
[26] http://en.wikipedia.org/wiki/Spam_%28electronic%29

or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spoofing can take place on the Internet in several different ways. One common method is through e-mail. E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message.

Another way spoofing takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions. Finally, spoofing can be done by simply faking an identity, such as an online username. For example, when posting on a Web discussion board, a user may pretend he is the representative for a certain company, when he actually has no association with the organization. In online chat rooms, users may fake their age, gender, and location. While the Internet is a great place to communicate with others, it can also be an easy place to fake an identity. Therefore, always make sure you know who you are communicating with before giving out private information.[27]

(e) OTHER TYPES OF CYBER CRIMES:

1. Cyber Terrorism:

Cyber Terrorism is “the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically.” Computers and the internet are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier. They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life. The tremendous role of computers stimulated criminals and terrorists to make it their preferred tool for attacking their targets. The internet has provided a virtual battlefield for countries having problems with each other such as Taiwan against China, Israel against Palestine, India against Pakistan, China against the US, and many other countries. This transformation in the methods of terrorism from traditional

[27] http://knowcybercrime121.blogspot.in/2010/05/spoofing.html

methods to electronic methods is becoming one of the biggest challenges to modern societies. In order to combat this type of terrorism a lot of effort should be done at the personal level, the country level, the regional level, as well as the international level to fight against this transnational type of crime. Cyber terrorism is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyber terrorism. [28]

A *narrower definition* of cyber terrorism could be, if cyber terrorism is treated similarly to traditional terrorism, then it only includes attacks that threaten property or lives, and can be defined as the leveraging of a target's computers and information, particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure.

There are some who say that cyber terrorism does not exist and is really a matter of hacking or information warfare. They disagree with labeling it terrorism because of the unlikelihood of the creation of fear, significant physical harm, or death in a population using electronic means, considering current attack and protective technologies. If a strict definition is assumed, then there have been no or almost no identifiable incidents of cyber terrorism, although there has been much public concern.

Cyber terrorism can also include attacks on Internet business, but when this is done for economic motivations rather than ideological, it is typically regarded as cybercrime.

Cyber terrorism is limited to actions by individuals, independent groups, or organizations. Any form of cyber warfare conducted by governments and states would be regulated and punishable under international law.

Types of cyber terror capability:

The following three levels of cyber terror capabilities are defined by Monterey group:

1) Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

2) Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

3) Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography).

[28] http://en.wikipedia.org/wiki/Cyberterrorism

Ability to create sophisticated hacking tools. Highly capable target analysis, command, control and organization learning capability.[29]

2. Software Piracy:

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium. Software piracy is illegal. Each pirated piece of software takes away from company profits, reducing funds for further software development initiatives. Ironically, many who pirate software are fully aware of the legalities, though they are able to rationalize continuing the practice. Some have difficulty understanding the distinction between freeware, shareware and commercial software. Others believe students won't be able to take advantage of the many technology-based educational opportunities without access to unaffordable software. Since software budgeting is often inadequate, and occasional upgrade of hardware makes older versions of software obsolete after several years, some think the only "solution" to the problem is to pirate newer versions of past purchased software. Finally, some people don't believe that software piracy is truly stealing because there is no loss of a tangible product involved in the act of piracy.[30]

3. Web Jacking:

In these kinds of offences the hacker gains access and control over the web site of another. There are many cases of web jacking, recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed on this website. This type of illegal treatment is mainly done to procure money.

[29] Ibid
[30] http://education.illinois.edu/wp/crime/piracy.htm

LEGAL ENACTMENTS

INTERNATIONAL LAWS AND ORGANIZATIONS ON CYBER CRIMES:

The International Organization on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies, a forum for the exchange of information concerning computer crime investigation and other computer related forensic issues. In response to the to the G-8 Communique and Actions plans of 1997, IOCE was tasked with the development of international standards for the exchange and recovery of electronic evidence. During the International Hi – Tech Crime and Forensics Conference (IHCFC) of October 1999, the IOCE held meetings and a workshop which reviewed the United Kingdom Good Practice Guide and the SWGDE Draft Standards. The working groups proposed the following principles, which were voted upon by the IOCE delegates present with unanimous approval.

The international principles developed by IOCE for the standardized recovery of computer based evidence are governed by the following attributes:

1) Consistency with all legal systems;

2) Allowance for the use of common language;

3) Durability;

4) Ability to cross international boundaries;

5) Ability to instil confidence in the integrity of evidence;

6) Applicability to all forensic evidence; and

7) Applicability at every level, including that of individual, agency, and country.[31]

International conventions:

The *Convention on Cybercrime*, also known as the Budapest *Convention on Cybercrime* or the *Budapest Convention*, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada and Japan.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature

[31]Barkha & U. Rama Mohan, Cyber Law & Crimes – IT Act 2000 & Computer Crime Analysis, New Ed. 2006, S. P. Gogia (H. U. F.) Publications, p. 5.

in Budapest, on 23 November 2001 and it entered into force on 1 July 2004.[3] As of November 2013, 41 states have ratified the convention; while a further 11 states had signed the convention but not ratified it.

On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivates by racism or xenophobia.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security.[6] It also contains a series of powers and procedures such as the search of computer networks and lawful interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

The Convention aims principally at:

1) Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime

2) Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form

3) Setting up a fast and effective regime of international cooperation

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighboring.

It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans-border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.

The Convention is the product of four years of work by European and international experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. Currently, cyber terrorism is also studied in the framework of the Convention.

The Convention was signed by Canada, Japan, the United States, and the Republic of South Africa on 23 November 2001, in Budapest. As of November 2013, the non-European states that have ratified the treaty are Australia, Dominican Republic, Japan, Mauritius, and the United States.

On October 21, 2013, The Foreign Ministry of Colombia through a press release stated the Council of Europe invited Colombia to adhere to the "Convention of Budapest". Colombia has not acceded to the convention.[32]

INDIAN LAWS GOVERNING CYBER CRIMES:

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology thus, *"INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000]* was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of *IT Amendment Act, 2008 [ITAA-2008]*.

The ITA-2000 defines '*Computer*' as *any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.* The word '*computer*' and *'computer system'* have been so widely defined and interpreted to mean *any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities;* and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

Scope and applicability:

The scope and applicability of ITA-2000 was increased by its amendment in 2008. The word *'communication devices*' inserted having an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video, etc. like what was later being marketed as iPad or other similar devices on Wi-fi and cellular models. Though ITA- 2000 defined 'digital signature', however said definition was incapable to cater needs of hour and therefore the term 'Electronic signature' was introduced and defined in the ITAA -2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

[32] http://en.wikipedia.org/wiki/Convention_on_Cybercrime

The new amendment has replaced Section 43 with Section 66. The Word "hacking" used in Section 66 of earlier Act has been removed and named as "data theft" in this section and has further been widened in the form of Sections 66A to 66F. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons' password or electronic signature, cheating by personation through computer resource or a communication device, publicly publishing the information about any person's location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under section 66 are cognizable and non-bailable. Whereas, the consequence of Section 43 of earlier Act were Civil in nature having its remedy in the form of damages and compensation only, but under Section 66 of the Amendment Act, if such act is done with criminal intention that is mens-rea, then it will attract criminal liability having remedy in imprisonment or fine or both.

Adjudication:

Adjudication powers and procedures have been dealt in Sections 46 and thereafter. As per the Act, the Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. Very few applications were received during first 10 years of existence of the ITA, that too in the major metros only. However, the trend of receiving complaint under ITA is rapidly growing. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level, has also been described in the Act. Every adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure.

The major Acts , which got amended after enactment of ITA:

1) The Indian Penal Code, 1860:

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above

amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463,464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

2) The Indian Evidence Act 1872:

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the Act.

3) The Bankers' Books Evidence (BBE) Act 1891:

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as: '"bankers ' books' include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data ...to retrieve data that is lost due to systemic failure or ....
The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

Issues not covered under ITA:

ITA and ITAA is though landmark first step and became mile-stone in the technological growth of the nation; however the existing law is not sufficed. Many issues in Cyber crime and many crimes are still left uncovered. Territorial Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cyber crime etc. Since cyber crimes are basically computer based crimes

and therefore if the mail of someone is hacked in one place by accused sitting far in another state, determination of concerned P.S., who will take cognizance is difficult. It is seen that the investigators generally try to avoid accepting such complaints on the grounds of jurisdiction. Since the cyber crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction; it is needed to proper training is to be given to all concerned players in the field.

Preservation of evidence is also big issue. It is obvious that while filing cases under IT Act, very often, chances to destroy the necessary easily as evidences may lie in some system like the intermediaries' computers or sometimes in the opponent's computer system too.
However, most of the cyber crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.[33]

Thus to conclude, society as of today is becoming more and more dependent upon technology and crime based on electronic offences are bound to increase. Endeavour of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of technology contains every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes.

Criticisms:

The amendment was passed in an eventful Parliamentary session on 23rd of December 2008 with no discussion in the House. Some of the cyber law observers have criticized the amendments on the ground of lack of legal and procedural safeguards to prevent violation of civil liberties of Indians. There have also been appreciation about the amendments from many observers because it addresses the issue of Cyber Security.

Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence. They can also secure assistance from computer personnel in decrypting data, under penalty of imprisonment.

Section 66A is widely criticized. It has led to numerous abuses reported by the press. Section 66A has also been criticised and challenged in Lucknow and Madras High Courts for its constitutional validity. Based on Section 66A, Bombay High Court has held that creating a website and storing false information on it can entail cyber crime.[34]

[33]http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective
[34] http://en.wikipedia.org/wiki/Information_Technology_Act_2000

Strengthening the IT Act:

1) The IT (Amendment) Act, 2008, reduced the quantum of punishment for a majority of cyber crimes. This needs to be rectified.

2) The majority of cyber crimes need to be made non-bailable offences.

3) The IT Act does not cover a majority of crimes committed through mobiles. This needs to be rectified.

4) A comprehensive data protection regime needs to be incorporated in the law to make it more effective.

5) Detailed legal regime needed to protect privacy of individuals and institutions.

6) Cyber war as an offence needs to be covered under the IT Act.

7) Parts of Section 66A of the IT Act are beyond the reasonable restrictions on freedom of speech and expression under the Constitution of India. These need to be removed to make the provisions legally sustainable.[35]

[35] http://www.dnaindia.com/scitech/report-india-s-information-technology-act-has-not-been-effective-in-checking-cyber-crime-expert-1818328

CONCLUSION & SUGGESTIONS

Cyber crime is one of the most deadliest and dangerous crimes of the world. Why the society is treating it as the most heinous crimes of all? It may be because the society now is ultra modernized. Each and every individual now depends on technology starting from pager to the internet, each one us are now using these technologies in one form or the other. This has given rise to the darker side of internet age.

Internet now has become a common tool of misuse. Though the topics covered in the preceding pages, this much is clear that the scope of cyber crime is very vast. This crime is not confined to one form but can degrade and cheat the society in hundreds of ways. Also its nature is like one of most deadly crime of the world. It's easy to commit but very difficult to mend. It's a crime of one of the most complex nature.

Indian society is now developing at a very fast pace and so is the advancement made in technological stature of society but with this technological advancement country is inviting equal amount of danger with it. Technology can be the recourses, but the country like Indian should think over its justification before adoption. This is a time to act, to plan, to get protected the generation, because electronic technology has greater potentiality to destroy society than any other previous variables. No doubt computer is providing us with lot of facilities, making our work easier but these facilities of computer technology have come with tones drawbacks, one such is cyber crime. Though it makes the life so speedy and fast, but hurled us under the black shadow of a menace which we popularly recognize as "cyber crime". It even posses the capacity to collapse the whole system within a fraction of seconds. Therefore, it is necessary to prevent this modern havoc from degrading the entire society.

Recommendations to prevent cyber crime:

It's a well known saying that **"**Prevention is always better than cure", therefore, it is always better to take certain precaution beforehand rather than regretting afterwards.

Whoever is accessing the net should keep in mind the following things:

1. Avoid disclosing any personal or confidential information so as to avoid getting being victim of cyber stalking. This is as good as disclosing your identity to strangers in public place.

2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3. Guard your computer against virus attacks by using new updated version of antivirus software.

4. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

5. Use firewalls to guard computer.

6. Web servers running public sites must be physically separate protected from internal corporate network.

7. Self protection should be your top priority.

8. Efforts should be made from all the three levels i.e. Individual, Government and private organizations. They all should try to protect state against such Illegal threat.

A major hurdle in cracking down on the perpetrators of cyber crimes such as hacking is the fact that most of them are not in India. The IT Act does give extra-territorial jurisdiction to law enforcement agencies, but such powers are largely inefficient. This is because India does not have reciprocity and extradition treaties with a large number of countries.

What India needs to do is to be a part of the international momentum against cyber crime. The only international treaty on this subject is the Council of Europe's Convention on Cyber Crime, formulated primarily by the European Union. By signing this treaty, member countries agree on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals.

At the last count, there are 43 member countries, including the US and South Africa. India is not yet a part of this group and being a member would go a long way in addressing this issue of cross-border cyber terrorism.

The Indian IT Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crime and criminals. "We are now beginning to see new categories and varieties of cyber crimes, which have not been addressed in the IT Act. This includes cyber stalking, cyber nuisance, cyber harassment, cyber defamation and the like. Another glaring omission in the Act, which contradicts the very objective of passing such a law - encouraging e-commerce by giving it legal validity — is the fact that the IT Act does not cover electronic payment. However, some steps such as amendments to the Negotiable Instruments Act have been taken to address this issue. Also in the making is a law on data protection.

BIBLIOGRAPHY

BOOKS:

1) Barkha & U. Rama Mohan, Cyber Law & Crimes – IT Act 2000 & Computer Crime Analysis, New Ed. 2006, S. P. Gogia (H. U. F.) Publications.

2) Edited by S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, ed. 2004, Published by Prof. (Ms.) S. K. Verma, Director, for Indian Law Institute, Bhagwandas Rd, New Delhi, and Printed at Shivam Offset Press, New Delhi.

WEBSITES:

1) http://www.crimeresearch.org/analytics/702/

2) www.directionsmerg.com

3) http://www.helplinelaw.com/docs/main.php3?id=CDII2

4) http://en.wikipedia.org/wiki/Digital_signature_forgery

5) http://cyberlawpioneers.com/index.php/cyber-pornography/

6) http://en.wikipedia.org/wiki/Cyberstalking

7) http://en.wikipedia.org/wiki/Internet_fraud

8) http://en.wikipedia.org/wiki/Financial_crimes

9) http://en.wikipedia.org/wiki/Online_gambling

10) http://en.wikipedia.org/wiki/Gambling_in_India

11)http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

12) http://en.wikipedia.org/wiki/Hacker_%28computer_security%29

13) http://ahmedccna.blogspot.in/2012/03/virus-dissemination.html

14)http://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

15) http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml

16) en.wikipedia.org/wiki/Steganography#Use_by_terrorists

17) http://en.wikipedia.org/wiki/Spam_%28electronic%29

18) http://knowcybercrime121.blogspot.in/2010/05/spoofing.html

19) http://en.wikipedia.org/wiki/Cyberterrorism

20) http://education.illinois.edu/wp/crime/piracy.htm

21) http://en.wikipedia.org/wiki/Convention_on_Cybercrime

22)http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

23) http://en.wikipedia.org/wiki/Information_Technology_Act_2000

24) http://www.dnaindia.com/scitech/report-india-s-information-technology-act-has-not-been-effective-in-checking-cyber-crime-expert-1818328