Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259

Cyber Crime in the Society: Problems and Preventions

Kamini Dashora, PhD, Principal, P.P. Patel College of Social Sciences, (Affiliated Sardar Patel University, Vidyanagar, Gujarat, India)

Abstract: *The world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind.*

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in society. This article is based on various reports from news media and news portal.

Keywords: Cyber crime, Hacking, Phishing, Cyber squatting

1. Introduction

Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crime depending on their nature and extent. One thing is certain, it is that a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence. Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

The term 'cyber crime' is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Before evaluating the concept of cyber crime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

2. Computer as a Tool

When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

3. Computer as a Target

These crimes are committed by a selected group of criminals. Unlike crimes using he computer as a tool, these crimes requires the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. But it is worth knowing that Africans and indeed Nigerians are yet to develop their technical knowledge to accommodate and perpetrate this kind of crime.

4. Conventional Crime

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.”The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin “the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences”. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

5. Cyber Crime

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

A generalized definition of cyber crime 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.

6. Distinction Between Conventional and Cyber Crime

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

7. Reasons for Cyber Crime

"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 crime. 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 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. **Complex:** 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. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
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 cyber criminal to gain access and control over the computer system.
5. **Loss of evidence:** Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

8. 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. Organised hackers

These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. 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 ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

4. Discontented employees

This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

9. Mode and Manner of Commiting Cyber Crime

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 2000 have no where used this term so to avoid any confusion we would not interchangeably use the word hacking for ‘unauthorized access’ as the latter has wide connotation.

Theft of information contained in electronic form: 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.

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.

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.

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.

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 (DDoss) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

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. Almost brought development of Internet to a complete halt.

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).

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.

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 crime.

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 the site of MIT (Ministry of Information Technology) 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 whereby control over the site of another is made backed by some consideration for it.

10. Classification

The subject of cyber crime may be broadly classified under the following three groups. They are-

1. Against Individuals

a. their person &
b. their property of an individual

2. Against Organization

a. Government
c. Firm, Company, Group of Individuals.

3. Against Society at large:

The following are the crimes, which can be committed against the followings group

Against Individuals: –
i. Harassment via e-mails.
ii. Cyber-stalking.
iii. Dissemination of obscene material.
iv. Defamation.
v. Unauthorized control/access over computer system.
vi. Indecent exposure
vii. Email spoofing
viii. Cheating & Fraud

Against Individual Property: -
i. Computer vandalism.
ii. Transmitting virus.
iii. Netrespass
iv. Unauthorized control/access over computer system.
v. Intellectual Property crimes
vi. Internet time thefts

Against Organization: -

i. Unauthorized control/access over computer system
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization.
iv. Distribution of pirated software etc.

Against Society at large: -

i. Pornography (basically child pornography).
ii. Polluting the youth through indecent exposure.
iii. Trafficking
iv. Financial crimes
v. Sale of illegal articles
vi. Online gambling
vii. Forgery

The above mentioned offences may discuss in brief as follows:

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 crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime 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.

10. 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.

11. 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 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.

11. 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 Information Technology Act deals with the various cyber crimes in chapters IX & XI. 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.

12. 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. "Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime". 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.

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 crime 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. 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. Furthermore, 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.

5. 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.

6. 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.

7. 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.

8. 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".

9. 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.

10. 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.

13. Prevention of Cyber Crime

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things

1. To prevent cyber stalking avoid disclosing any information pertaining to one self. 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. Always use latest and update antivirus software to guard against virus attacks.
4. always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to

the site as leaving the cookies unguarded might prove fatal.

8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network. Adjudication of a Cyber Crime - 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.

14. Conclusion

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime 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 check crime. Undoubtedly the Act is a historical step in the cyber world. Further I all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime. I 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.

References

Cyber Crime Today &Tomorrow, Thiru DayanithiMaran

Cyber crime Up Police found wanting, *Chandigarh Tribune* Monday May 28, 2001.

Cyber Crimes on the rise in state - Kerala: *The Hindu* Monday Oct 30, 2006.

Duggal Pawan - Is this Treaty a Treat?

Duggal Pawan – The Internet: Legal Dimensions

Duggal Pawan - Cybercrime

Kapoor G.V. - Byte by Byte

Kolkata man threatens to blow up Stock exchanges arrested. Express India.com

Kumar Vinod – Winning the Battle against Cyber Crime

Mehta Dewang- Role of Police in Tackling Internet Crimes

Nagpal R- Defining Cyber Terrorism

Nagpal R. – What is Cyber Crime?

Nasik Police play big boss for internet voyeurs, *Hindustan Times*, Sunday, Oct 28, 2007.
Nowa Pune base for net's cyber cops *The Hindu* Sunday Nov 26 2006.

Police make headway, *The Hindu*, Sunday October 29.2006.

Suhas Shetty Cyber Crime Case, First conviction in India under ITA-2000.

Tamil Nadu to come out with IT security policy soon, *The Hindu*, Saturday, Oct 27, 2007.

Youth in jail for sending email threat, *The Hindu* Friday August 10, 2007.