ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Cyber Crime

**P. Chaitanya Reddy**
**B.Tech Student,**
**Sphoorthy Engineering College, Hyderabad.**

**Mr. T. Pavan Kumar**
**Assistant Professor**
**Sphoorthy Engineering College, Hyderabad.**

**Mrs. J. Deepthi (Ms. B.Tech)**
**HOD**
**Sphoorthy Engineering College, Hyderabad.**

## 1. Introduction:

The term cybercrime is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cybercrime 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 cybercrime 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.

### 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.

### CYBERCRIME

Cybercrime is the latest and perhaps the most complicated problem in the cyber world. 'Cybercrime 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 cybercrime'.

A generalized definition of cybercrime 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 diddling, salami attacks, logic bombs,

Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

## 2. REASONS FOR CYBERCRIME:

Hart in his work 'The Concept of Law' has said "human beings are vulnerable so rule of law is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 cybercrime. The reasons for the vulnerability of computers may be said to be:

**a) Capacity to store data in comparatively small space**

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

**b) Easy to access**

The problem encountered in guarding a computer system from unauthorized 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 canfool biometric systems and bypass firewalls can be utilized to get past many a security system.

**c) 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.

**d) 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.

**e) 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.

## 3. 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

**a) Children and adolescents between the age group of 12 – 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.

**b) Organized hackers-**

These kinds of hackers are mostly organized 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.

**c) Professional hackers /crackers**

Their work is motivated by the color 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 loophole.

**d) 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.

## 4. MODE AND MANNER OF COMMITING CYBERCRIME

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

### 4.1 Unauthorized access to computer systems or networks / Hacking

This kind of offence is normally referred as hacking in the generic sense. However the framers of the information technology act 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.

4.2 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

### 4.3 Email bombing

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

### 4.4 Data diddling

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

### 4.5 Salami attacks

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

### 4.6 Denial of Service attack

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

### 4.7 Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe.

The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. Almost brought development of Internet to a complete halt.

### 4.8 Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

### 4.9 Trojan attacks

This term has its origin in the word „Trojan horse". In software field this means an unauthorized program, which passively gains control over another's system by representing itself as an authorized program. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

### 4.10 Internet time thefts

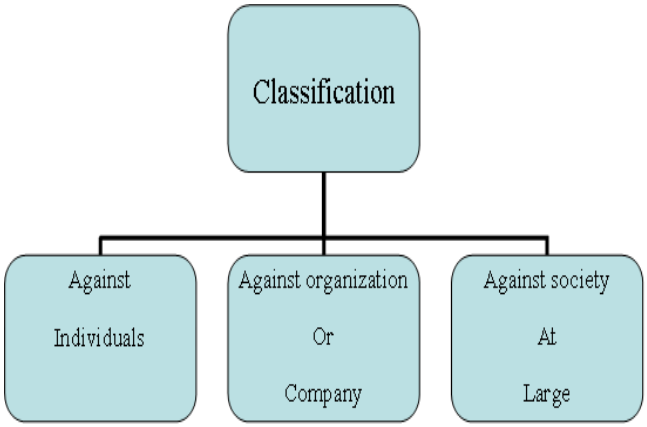
Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajw's case- the Internet hours were used up by any other person. This was perhaps one of the first reported cases related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

### 4.11 Web jacking

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently 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 where by control over the site of another is made backed by some consideration for it.

## 5. CLASSIFICATION:

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




### 5.1 Against Individuals:

- Harassment via e-mails.
- Cyber-stalking.
- Dissemination of obscene material.
- Defamation.
- Unauthorized control/access over computer system.
- Indecent exposure
- Email spoofing
- Cheating & Fraud

### 5.1Against Individual Property:

- Computer vandalism.
- Transmitting virus.
- Unauthorized control/access over computer system.
- Intellectual Property crimes
- Internet time thefts

### 5.2 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.

### 5.3 Against Society at large:

- Pornography (basically child pornography).
- Polluting the youth through indecent exposure.
- Trafficking
- Financial crimes
- Sale of illegal articles
- Online gambling
- Forgery

The above mentioned offences may discussed in brief as follows:

### a) 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

**b) 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.

**c) Dissemination of obscene material/ 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.

**d) 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.

**e) 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.

**f) 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.

**g) 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.

**h) 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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**.**

### i) 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 cybercrime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cybercrime 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 deploymentsystem* 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

- Putting the public or any section of the public in fear; or
- Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or
- 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.

### j) 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.

### h) 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.

## 6. SOME CASES STUDIES:

### 1. Pune Citi bank MphasiS Call Center Fraud

US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we can not ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud.

They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The call center employees are checked when they go in and out so they can not copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history.

Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

### 2. Parliament Attack Case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents.

The laptop contained several evidences that confirmed of the two terrorists‟ motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftily made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

### 3. Andhra Pradesh Tax Case-

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted.

It later revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax.

### 4. Baazee.com case

CEO of Baazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail.

This opened up the question as to what kind of distinction do we draw between Internet Service

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider.

It also raises a lot of issues regarding how the police should handle the cybercrime cases and a lot of education is required.

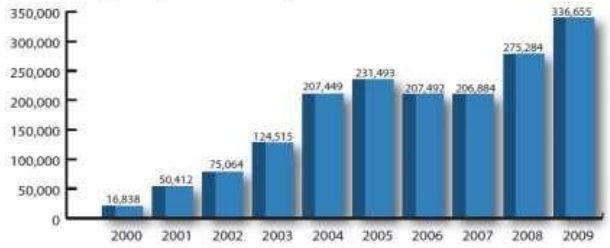
## SELECTED ASIA / PACIFIC CASES:

The following section provides a selection of actions taken against file-sharing Web sites and P2P services in the Asia/Pacific region, focusing on Australia, China, Japan and South Korea.

- In Australias largest copyright infringement case, three university students received criminal sentences for running a Web site called MP3/WMA Land, which offered more than 1,800 pirated songs for download. In light of their age at the time and the fact that they never profited from their actions, the court warranted 18-month suspended sentences for two of the students and an additional fine of US$5,000 for one of them.
- Reportedly, China has become a leading exporter of counterfeit and pirated goods to the world. The U.S. industry estimates the value of counterfeit goods in China at US$19 billion to US$24 billion, with losses to U.S. companies exceeding US$1.8 billion a year. The severe piracy problems derive from a combination of cultural, historic and economic factors and are further aggravated by inconsistent, weak enforcement by officials. Filesharing Web sites and networks such as Jelawat and Kuro have been developing rapidly, too. The distributors of P2P software claim that file-sharing falls within the private use exception to copyright, but the Supreme Peoples Court of China rejected this interpretation. Increasingly, copyright owners and right organizations are challenging file-sharing Web sites on copyright infringement claims.

## Statistical data on Cybercrime:

Figure 1: Yearly Comparison of Complaints Received via the IC3 Web site




## Snapshot of Important Cyberlaw Provisions in India

| Offence | Section under IT Act |
|---|---|
| Tampering with Computer source documents | Sec.65 |
| Hacking with Computer systems, Data alteration | Sec.66 |
| Publishing obscene information | Sec.67 |
| Un-authorized access to protected system | Sec.70 |
| Breach of Confidentiality and Privacy | Sec.72 |
| Publishing false digital signature certificates | Sec.73 |

## Computer Related Crimes Covered under Indian Penal Code and Special Laws

| Offence | Section |
|---|---|
| Sending threatening messages by email | Sec 503 IPC |
| Sending defamatory messages by email | Sec 499 IPC |
| Forgery of electronic records | Sec 463 IPC |
| Bogus websites, cyber frauds | Sec 420 IPC |
| Email spoofing | Sec 463 IPC |
| Web-Jacking | Sec 383 IPC |
| E-Mail Abuse | Sec 500 IPC |
| Online sale of Drugs | NDPS Act |

## 7.PREVENTION OF CYBERCRIME:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. One should make this his part of cyber life. Mr. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the **5P** mantra for online security*: **Precaution, Prevention, Protection,Preservation and***

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

***Perseverance.*** A citizen should keep in mind the following things

- To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and up date anti virus software to guard against virus attacks
- Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- Use of firewalls may be beneficial. They provide access to only known users, or people who the user permits.
- Web servers running public sites must be physically separate protected from internal corporate network.

## 8. CONCLUSION:

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime 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 cybercrime.

However, a lot of work has to be done in this field. Just as human mind is ingenious enough to devise new ways for perpetuating crime, similarly, human ingenuity needs to be channelized into developing effective legal and regulatory mechanisms to control and prevent Cybercrimes.

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:

1. http://cyberlaws.net/cyberindia/articles.htm
2. http://www.cyberlawsindia.net/
3. http://satheeshgnair.blogspot.com/2009/06/se le cted-case-studies-on-cyber-crime.html
4. http://www.cybercellmumbai.com/
5. Kumar Vinod – Winning the Battle against Cybercrime
6. www.wikisedia.com
7. www.pediain.com