"CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY"

NEELESH JAIN[1], VIBHASH SHRIVASTAVA[2]

[1]Professor
[2]Assistant Professor
Department of Computer Applications,
Sagar Institute of Research and Technology, Bhopal (MP) India

Abstract

The Internet is often described as a wonderful tool, an engaging place and a liberating experience…… but for whom? There is the potential for many of us to become victims to the growing pool of criminals who skilfully navigate the Net. Cyberspace often known as Web is an environment that is intangible and dynamic.This paper argues that Cyber Crime or e – crime presents a new form of business and Hi-tech Criminals.

This paper explores an overview of Cyber Crimes, the cyber-crime perpetrators and their motivations also I want to discuss in detail of different cyber crimes, and unique challenges and response issue which may be encountered during the prevention, detection and investigation and also outlined the different section of IT Act 2000 of India also proposed new provision in IT Act 2000.

Keywords
Cybercrime, Hackers, Crackers, Child Pornography, Viruses, Worms, Trojans, Cyberstalking, Cyber Defamation, Cyber Law, India, IT Act 2000.

1. Introduction

The Internet changes everything. It's upset our notions of how things should be, how countries should be governed, how companies should be run, how teachers teach and children learn, and even how housewives make new recipes. It mixes up our conceptual framework of what we think we know about the world, about each other and about ourselves. It is liberating, exciting, challenging and terrifying all at the same time.. To a majority of the people, the Internet remains mysterious, forbidding, incomprehensible and frightening.

Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities. As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few. Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve. At the same time, legislators face the need to balance the competing interests

[1] Opp. Barrister Ki Dant, Lajpartpura Ward, Sagar, Madhya Pradesh, India, 470002, Tel No 91-7582-244901.

[2] 69, Shanichary Ward, One Way Parkota Road Sagar, Madhya Pradesh, India, 470002, Tel No. 91- 9329738680.

between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.

Further complicating cyber crime enforcement is the area of Legal Jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of Internet crime without cooperation from other nations. Law enforcement agencies around the world are working together to develop new partnership, new forensic methodologies and new responses to cyber crime in order to ensure safety and security on the Internet.

Due to its global dimensions and borderless nature, new and innovative responses are required to the issue of cybercrime or e-crime or computer crime. However, this paper argues that e-crime, and particularly 'hi-tech crime', presents a new form of business that will require a fundamental paradigm shift in policing.

In section 2 and 3 of this article, we begin by providing an overview of cybercrimes, and cybercrimes perpetrators and their motivations. Then in Section 4 we have discuss the different type of cybercrimes and then in Section 5 we identified and discuss the new and unique challenges and response issued which may e encountered during the prevention, detection and investigation of such crimes and further in Section 6 and 7 we outline what IT Act 2000 of India is doing to prevent and reduce the incident of this type of crime and enhance the safety and security f our communities. In Section 8, we proposed the changes in IT Act 2000 and finally, we conclude this paper with a brief statement on the cybercrime and its challenges.

2. Background

What is the Cyber Crime? Some experts believe that cyber-crime is nothing more than ordinary crime committed by high tech computers where computer is either a tool or target or both and other experts view that cyber-crime is a new category of crime requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime do not deal with such as jurisdiction, international cooperation, intent and the difficulty of identifying the perpetrator.

2.1 The Perpetrators – Hackers & Crackers

2.1.1 *Hackers*

Hacker is a term commonly applied to a "Computer use who intends to gain unauthorized access to a computer system." According to IT Act 2000 section 66 a person whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects its inuriously by any means is a hacker.

2.1.2 *Crackers*

A "cracker" is a hacker with criminal intent. According to the Jargon Dictionary[3] this term is used to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers maliciously sabotage computers, steal information located on secure computers and cause disruption to the networks for personal or political motives.

[3] The Jargon dictionary on website http://www.netmeg.net/jargon/terms/c/cracker.html.

3. Why People Hack.

Cyber Crime presents as a "*new form of business*", will be characterized by new forms of crime, a far broader scope and scale of offending and victimisation, the need to respond in much more timely way, and challenging technical and legal complexities. So hacking involve different personal, political or professional motives.

3.1 Hactivism

In recent years it is seen that Hacktivists launch business motivated attacks on public web pages or e-mail servers. The hacking groups and individuals, or hacitivists overload email servers by sending massive amounts of e-mails to one address and hack into websites to send a professional or business messages.

3.2 Employees

In a study it is found that disgruntled employees are the greatest threat to a computer security. Employees steal confidential information and trade secrets for the financial benefits. According CBI (Cyber crime cell) disgruntled insiders are a major source of computer crimes. Insiders do not need a great deal of knowledge about their target computers, because their inside knowledge of the victim's system allows them unrestricted access to cause damage to the system or to steal system data.

3.3 Recreational Hackers

"Recreational hackers" break into computer networks for the thrill of the challenge or for bragging rights in the hacking community. The recreational hacker download attack script and protocols from the Internet only and launch them against the victim sites with little knowledge of the systems they are attacking.

3.4 Web site Administrators and Web Pages.

Websites also access a lot of hidden background information from the user. The remote website can determine the following important information about the visitor;

a. the IP address the user is accessing the web site from;
b. the number of prior visits to the web site, and the dates;
c. the URL of the page that contained the link to get the user to the web site;
d. the user's browser type and operating system and version;
e. the user's screen resolution;
f. whether JavaScript and VBScript are enabled on the user's computer;
g. how many web pages the user has visited in the current session;
h. the local time and date; and
i. FTP username and password, if there is one.

4. Types of Cyber Crime

A computer is an indispensable tool for almost all cybe-crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply.

A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense. The different uses of computer will results to the criminal statutes.

When a computer is the target of the offense, the criminal goal is to steal information from, or cause damage to, a computer, computer system, or computer network. Hacking, cracking, espionage, cyberwarfare, and malicious computer viruses are

common forms of crimes that target the computer. The perpetrators may be teenage, students, professional or the terrorists.

The computer may also be the tool of the offense. The cyber criminals uses the computer to commit a traditional crime such as to print fake currency using advanced color printers.

Computers can also be incidental to the offense, but are nevetheless important because they contain the evidence of a crime. For example Child pornographer' computers may contain the produced, possessed, received, and/or distributed child pornography. Money Launderers, may use a computer to store details of their laundering operation instead of relying on paper accounting records.

4.1 Malicious Code – Viruses, Worms and Trojans

4.1.1 Viruses

A virus is a program that modifies other computer programs. These modifications ensure that the infected program replicates the virus. Not all viruses cause damage to its host. A virus is typically spread form one computer to another by e-mail, or infected disk. However a virus cannot infect another computer until the program is executed. A common method of virus execution is when a computer user is tricked into opening a file attacked to an e-mail, thinking the file is a harmless program coming from a friendly source. The most popular example of virus is the Melissa virus which was launched in March 1999. The Melissa virus was hidden in a Microsoft word attachment that appeared to come from a person knows to the recipient. The program activated a macro that tread the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses. The virus was estimated to have caused $80 million in damages.

4.1.2 Worms

A worm is stand alone program that replicates itself. A worm can wind its way throughout a network system without the need to be atttached to a file, unlike viruses. For example I loveYou worm in 2001 was estimated the loss caused to be $US 10.7 billion.

4.1.3 Trojan Horses

A Trojan Horses is a an innocent looking computer program that contains hidden functions. Theyloaded onto the computer's hard drive an executed along with the regular program. However, hidden in the innocent program is a sub-program that will perform an unauthorized function. A Trojan horse is the most common way in which viruses are introduced int computer systems. For example Back Orifice 2000 is a program designed for misuse and attack on another computer

4.2 Denial of Service

A Denial of Service ("DoS") is an attack or intrusion designed for use against computers connected to the Internet whereby one user can deny service to other legitimate users simply by flooding the site with so much traffic that no other traffic that no other traffic that no other traffc can get in or out. The hacker isn't necessarily trying to break in to the system or steal data data but rather just prevent users from accessing their own network for reasons only the hacker knows; revenge, ecnomical or political gain, or just plain nastiness. For example in Feb 2000, a fifteen year old canadian boy known as "MafiaBoy" allegedly used a DoS attack to shut down popular interest sites such Yahoo, Amazon.com, Buy.com and others.

4.3 Cyberstalking

Cyber stalking is when a person is followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened. Stalking or being 'followed' are problems that many people, especially women, are familiar with. Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. The internet mirrors the real world. That means it also reflects real life & real people with real problems. Although it is rare, Cyber stalking does occur. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. A cyber stalker does not have to leave his home to find, or harass his targets, and has no fear of physical violence since he believes he cannot be physically touched in cyberspace. He maybe may be on the other side of the earth or a neighbour or even a relative! And a stalker could be of either sex.

Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female, but sometimes men are also stalked. The figures are more on assumed basis and the actual figures can really never be known since most crimes of such natures go unreported.

4.4 Financial crimes

This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

4.5 Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). Recent Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple for pornography.

4.6 Sale of illegal articles

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

4.7 Online gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

4.8 Intellectual Property crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

4.9 Email spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Pooja has an e-mail address pooja@asianlaws.org. Her enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

4.10Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

4.11Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

In a recent occurrence, Surekha (names of people have been changed), a young girl was about to be married to Suraj. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant. Then, one day when she met Suraj, he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about Surekha's character. Some of them spoke of affairs, which she had had in the past. He told her 168 that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, Suraj was able to prevail upon his parents and the other elders of his house to approach

the police instead of blindly believing what was contained in the mails. During investigation, it was revealed that the person sending those e-mails was none other than Surekha's stepfather. He had sent these e-mails so as to break up the marriage. The girl's marriage would have caused him to lose control of her property of which he was the guardian till she got married. Another famous case of cyber defamation occurred in America. All friends and relatives of a lady were beset with obscene e-mail messages appearing to originate from her account. These mails were giving the lady in question a bad name among her friends. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing them had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene e-mails they also put up websites about her, that basically maligned her character and sent e-mails to her family and friends containing matter defaming her.

5. Unique Challenges

As traditional criminals will use the computer technology, the nature and features of the cyber crime will bring new challenges for the Indian Government and policy makers due to;

- Anonymity;
- Global reach (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimization);
- The speed at which crimes can be committed;
- The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints, trace evidence or DNA; and
- The high cost of Investigations.

The challenges of the digital age and for the investigation of electronic crime or cyber crime or computer crime are numerous and diverse, and include;

- Bridging multi-jurisdictional boundaries;
- Retaining and preserving evidence;
- Acquiring appropriate powers;
- Decoding encryption;
- Proving Identity;
- Knowing where to look for evidence;
- Tackling the tools of crime and developing tools to counter crime;
- Rethinking the costs and priorities of investigations;
- Responding to crime in real time;
- Coordinating investigative activities;
- Improving training at all levels of the organization;
- Developing strategic partnerships and alliances;
- Improving the reporting of electronic crime;
- Enhancing the exchange of information and intelligence;
- Acquiring. Developing and retaining specialist staff; and
- Avoiding ‘tech-lag’ (or getting access to cutting edge technology).

The forensic challenges, in particular, are too considerable. The US Department of Justice in a report (2001, p.23) identifies four major challenges in relation to forensic evidence collection and analysis;

- **Finding evidence in the 'information ocean'** – Finding important evidence can be nearly impossible. Separating valuablexz1 ` 1232 information from irrelevant information also requires extraordinary technical efforts. Determining the location where evidence is stored can also be quite difficult.
- **Anonymity** – Computer networks permit persons to easily maintain anonymity and most web servers have a 'handle', a false name or identity.
- **Traceability** – Related to anonymity, traceability refers to how difficult it is to establish the source and destination of communications on computers and communication networks, such Internet. Traceability is becoming even more difficult because of the proliferation and easy availability for multiple communications providers. Communications on the Internet, for example, can easily pass through 10 different Internet Service Providers (ISP's), each of which must provide information to trace a communication.
- **Encryption** – Shortly, the vast majority of data and communications will be encrypted. Encryption can hinder law enforcement investigations and increase costs because of the problems associated with cracking the encryption.

6. Cyber Laws in India

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.

This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below:

- **Chapter-II** of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
- **Chapter-III** of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is –
    - Rendered or made available in an electronic form; and
    - Accessible so as to be usable for a subsequent reference

  The said chapter also details the legal recognition of Digital Signatures.

- **Chapter-IV** of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.
- **Chapter-V** of the act gives the idea of secure electronic records and secure digital signatures
- **Chapter-VI** of the act gives the rules, regulation, functions & procedure of the certifying authorities
- **Chapter-VII** of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.
- **Chapter-VIII** of the act talks about the duties of the subscribers.
- **Chapter-IX** of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of State Government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.
- **Chapter-X** of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.
- **Chapter-XI** of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.
- The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

7. Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

8. Proposed Changes in IT Act 2000

It is found that there should be the provision for the following –

a. Trap and Trace orders. The new IT Act should make such legislation that it is easier for cyber investigators to obtain "trap and trace" orders. "Trap and trace devices are used to capture incoming IP packets to identify the packet's origins. Due to the ease with which hackers are able to "spoof" their true origin, the most effective way to reconstruct the path of a virus, DoS or hacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrived at each individual router or server. In a case of single telephone company, it has been relatively easy for investigators to obtain trap and trace orders but today one communication is being carried by

several different {ISPs}, by one or more telephone company or one or more cell company and very soon by one or more satellite company. Once the segment of the route goes beyond the court's jurisdiction, investigators must then go the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace an on-line communication from start to finish.

b. We proposed new legislation such that makes young perpetrators fifteen years of age and older eligible for offences in serious computer crime.
c. The Cyber Cafes, Computer Training Centre, and other Institute where computer is the mode of training should be incorporated under some act.

9. Conclusion

Criminal behavior on the Internet, or cyber crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge.

Law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cyber crime in order to ensure safety and security on the Internet.

New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent and respond to cybercrime. This 'new business' will be characterized by new forms of crime, a far broader scope and scale of offending and victimisation, the need to respond in much more timely way, and challenging technical and legal complexities. Innovative responses such as the creation of 'cybercops', 'cybercourts' and 'cyberjudges' may eventually required to overcome the significant jurisdictional issues.

References

1. Etter,B. (2001), *The forensic challenges of E-Crime,* Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.
2. Etter B. (2002), *The challenges of Policing Cyberspace,* presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.
3. Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), *A Practical Approach to the Application of Federal Computer Crime Laws,* Santa Clara University, Vol 16, Number 2.
4. Gengler, B. (2001), *Virus Cost hit $20bn,* The Australian, 11 September p.36.
5. The IT Act 2000.
6. Cyber stalking India, www.indianchild.com.
7. Cyber crime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27 IST
8. Richard Raysman & Peter Brown (1999), *Viruses Worms, and other Destructive Forces* N. Y. L. J.

9. Kabay, M. E. (2000). *Studies and Surveys of Computer Crime,* Focus. http://securityportal.com/cover/coverstory2001211.html
10. KPMG (2000) , *E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation,* USA
11. Legard, D (2001), *Hackers Hit Government Sites,* Computer World, Vol 24 No. 26, 29 Jan, p.12.
12. Russell G. Smith, Peter Grabosky and Grgor Urbas, 0521840473 – *Cyber Criminals on Trial*, Cambridge University Press.
13. Seamus O Clardhuanin (2004), An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1
14. International crime and Cyber Terrorism, http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp.
15. Visited www.cbi.nic.in.