CHAPTER TWO

REVIEW OF LITERATURE

2.1 History and Development
2.2 Cyber Crime at World Wide
2.3 Review of Literature
2.1 HISTORY AND DEVELOPMENT:

Invention, development, marketing and ubiquitous utilization of digitizing technologies -- those which convert textual, auditory, and graphical information into, or from, binary sets and streams of data has made possible and inevitable, the Information Age. At the heart of ongoing technological change is the Internet, the foundation for worldwide computer networking and the purported Global Information Infrastructure. Today there are over 16 million home pages on the World Wide Web and approximately 70 million Internet users in 200 nations.

Computers and the Internet can offer great benefits to society. However, they can also present opportunities for crime, most of which are traditional crimes using new technology tools. The first recorded computer abuse occurred in 1958, and the first federally prosecuted case of cyber crime (involving the alteration of bank records by computer) was in 1966. During that and subsequent prosecutions, the internet was for a long time conceived as mere avenue to commit white-collar crimes such as fraud or embezzlement.

This rate of technological change, the spread of computer literacy and the growth of e-Commerce collaboration, such as alliances and marketplaces, make the challenge of restricting cyber-crime damage daunting.

At one extreme, cyber crime may mean nothing more than a fabricated term to describe what may (or may not) be actual changes in the amount and variations of computer crime and other forms of crime. At another extreme, cyber crime may represent one of many terms seemingly being used in attempts to articulate an emerging crime paradigm in which, by virtue of increasing use of computer and other digitizing technologies (i.e., as the result of computerization or perhaps more accurately, digitization).
Hence, cyber crime, as the term implies, involves substantial use of digitizing technology in order to commit old and new forms of conventional crime and computer crime at least partially within or through the realm of cyberspace.

Also, cyber crime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences.

2.2 CYBER CRIME AT WORLD WIDE:

Although the Internet may be considered the greatest achievement of the past 50 years, the technology behind it has created a sanctuary for various types of computer criminals. The unfortunate and ugly truth is that the Web is providing a brand new "world" where international cyber criminals can thrive, and the world's numerous criminal justice systems just aren't ready to address these crimes in their entirety.

Cyber criminals don't necessarily need to leave the comfort of their homes to commit their crimes. Today, for example, bank robberies can be committed in Southeast Asia via a computer that's being controlled by an individual in Russia. Identity theft is achieved through a complex network of individuals residing in North America, Europe, and Africa, all effectively working together on the Internet to profit from shared information. And organized crime has ties to spam campaigns, identity theft, denial-of-service attacks, and organized hacking rings.

The fact is that Internet crimes are almost always international crimes. When you read about a bank system being hacked in order to steal 100,000 accounts, more than likely this crime was committed by perpetrators overseas, and there will almost definitely be a connection to organized crime. This part of the story is rarely conveyed to the everyday reader, but it is critical to understand this fact if we are going to fix the problem.
In the world of cyber crime, law enforcement officials in most countries have recognized that they must move much faster than the average investigator due to the fact that computer evidence can “disappear” rather quickly. These same cyber investigators realize they must be willing and ready to cooperate with law enforcement officials in other countries if they actually plan to capture the Internet criminals. Laws, treaties, and conventions, such as the Convention on Cyber crime, have attempted to address the international cooperation issue. Although the Convention on Cyber crime is an outstanding step in the right direction, is not a “law” that applies to all countries. Regardless of whether the country is a member of this Convention, the punishments levied are based on the local laws of the land.

But the problem with investigating international cyber crimes and capturing criminals on the Internet is not necessarily due to lack of cooperation among international law enforcement bodies. The issue has much more to do with the fact that the legal systems throughout the world vary greatly and take a very long time to change. These two facts make it extremely difficult for law enforcement to cooperate, investigate, capture, and ultimately prosecute the cyber criminals today. If we accept the fact that the greatest hurdle in arresting international cyber criminals is that various legal systems just aren’t prepared to address the speed at which these crimes occur or the various nuances that are unique to computer crimes, then the question is: What can we do to fix the problem?

It’s obvious that the Internet requires some type of governance. But it is just as obvious that trying to establish this governance through the numerous legal systems might not be practical. The other possibility for governing the Internet, and, more specifically, the criminal activity that occurs on the Internet, would be to change the structure of the Internet.
Although I don’t support ideas like the “national firewalls” put in place by some countries, this type of solution does afford some level of control over Internet traffic flowing through said country.

However, knowing all the possibilities with disguising or “spoofing” one’s information on the Web, I’m not sure that there is a way to truly “protect our borders” when it comes to the Internet. The solution might be to establish two Internets — the current Internet and a new, more secure Internet where users would be required to register prior to gaining access. Once again, though, we’re confronted with the issue of what would be the governing body that would manage the user registrations? Would it be an organization similar to the IANA (Internet Assigned Numbers Authority) or InterNIC that would manage user registrations on the “new” Internet, or do we need to establish an entirely new entity to manage a more secure Internet?

The fight against international cyber crime is going to take a concerted effort from large and small corporations, law enforcement in all countries, as well as the governments and legislative bodies of those same countries. Most importantly, the average end user will have to join the fight to bring about change on the Internet, or create a “new” Internet using the lessons we’ve learned.

2.3 REVIEW OF LITERATURE:

In this Chapter, a critical review of the literature concerning this research, published and unpublished is presented, since academicians, researchers and professionals have contributed very limited thought-provoking studies which come in the form of books and articles. Following are the previous research studies; those are related to the present research study.
• G. Rathinasabapathy (1991) : Cyber Crimes and Information Frauds: EMERGING CHALLENGES FOR PROFESSIONALS

In his published book author has concentrated on rapid raise in cyber crimes. Cyber crime which is also known as 'Internet crimes' or 'Computer crimes' is any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes or offences or contraventions under any law. Major cyber crimes reported in India are denial of services, defacement of web sites, spam, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. Further, most of the big libraries especially academic libraries are now have various kinds of networks like Local Area Network, Wide Area Network, etc. Library services are also being offered in networked digital environment. The author has also briefed about cyber crimes, its relevance and various ways to prevent cyber crimes. Computer-related crime, in particular cyber crime such as phishing and its progeny, require a different solution due to the non-terrestrial and non-territorial nature of electronic transactions. In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized. In order for there to be an effective global system to deal with the problem of computer-related crimes, there must be a multifaceted and multipronged approach using a combination of both legally coercive and non-legal measures.

'Prevention is better than cure' is not only meant for human health but for computers as well. It is always better to take necessary steps to prevent cyber crimes. Cyber crimes in India are slowly evolving from a simple e-mail crime to more serious Crimes like hacking and source code theft. It is a known fact that given the unrestricted number of free Web sites, the Internet is undeniably open to exploitation. cases of spam, hacking, cyber stalking and email fraud are rampant and, although cyber crimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness.[1]
CHAPTER TWO REVIEW OF LITERATURE

This paper gives the message to the Researcher, how “prevention is better than cure” for Cyber Crimes.

• Jerry Kang (2000): University of California, Los Angeles - School of Law, In their paper entitled as “Cyber-Race”, presented at Harvard Law Review, Vol. 113, p. 1131, 2000 as per their opinion they thought that, most inquiries into race and cyberspace have focused on the "digital divide" - whether racial minorities have access to advanced computing-communication technologies. Can cyberspace change the way that race functions in American society? He argues that cyberspace can disrupt racial schemas because it alters the architecture of both identity presentation and social interaction. Thus, cyberspace presents society with three design options: abolition, integration, and transmutation. After analyzing each option's merits, Professor Kang concludes that society need not adopt a single, uniform design strategy for all of cyberspace. Instead, society can embrace a policy of digital diversification, which explicitly zones different cyber spaces according to different racial environments. Although cyberspace is no panacea for the racial conflicts and inequality that persist, it offers new possibilities for furthering racial justice that should not be wasted [2].

This paper helps to the researcher how the society divided digitally by the use of Net.

• Patricia Brumfield(2000): Compilation of Cyber Laws (A Preliminary Analysis of federal and State Electronic Commerce Laws). The author gives memorandum containing preliminary examination of the impact of the federal legislation on electronic commerce on existing and future state law. The author gives details such as house of congress have approveds.761, titled the Electronic Signatures in Global and National Commerce Act or "E-Sign," and it was signed by the President on June 30, 2000, 18 States have enacted the Uniform Electronic Transactions Act (UETA), and it is pending in at least another ten. The
Uniform Electronic Transactions Act was approved by the National Conference of Commissioners on Uniform State Laws at its Annual Meeting in July 1999 as a body of legislation validating the use of electronic records and electronic signatures. The two pieces of legislation overlap significantly. The author says that Questions have been raised concerning the impact of E-Sign on the Uniform Electronic Transactions Act [3].

This is relevant to present study undertaken by the researcher as it deals with cyber crime.

- Abraham D. Sofaer, Seymour E. Goodman, Mariano-Florentino Cuéllar, Ekaterina A. Drozdova, David D. Elliott, Gregory D. Grove, Stephen J. Lukasik, Tonya L. Putnam, George D. Wilson (August 2000): The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP), in their paper entitled as "International Convention on Cyber Crime and Terrorism"; they conclude that, the information infrastructure is increasingly under attack by cyber criminals. The number, cost, and sophistication of attacks are increasing at alarming rates. Worldwide aggregate annual damage from attacks is now measured in billions of U.S. dollars. Attacks threaten the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information. Measures thus far adopted by the private and public sectors have not provided an adequate level of security. Investigations have been slow and difficult to coordinate. Some attacks are from States that lack adequate laws governing deliberate destructive conduct. Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple States. A clear consensus emerged that greater international cooperation is required, and considerable agreement that a multilateral treaty focuses on criminal abuse of cyber systems would help build the necessary cooperative framework. This monograph
summarizes and presents the Stanford Draft International Convention to Enhance Security from Cyber Crime and Terrorism and commentary on the Draft. The Draft acknowledges and builds upon the draft Convention on Cyber Crime proposed by the Council of Europe [4].

This concept of CRISP throws light on the problem of jurisdiction in Cyber Crime.

• Neal Kumar Katyal (April 2001) : Georgetown University Law Center, in their paper entitled as “Criminal Law in Cyberspace ”, presented at University of Pennsylvania Law Review, Vol. 149, April 2001 as per their opinion they thought that, the ILOVEYOU computer worm and the denial of service attacks on Yahoo, eBay, and ETrade, suggest that a new form of crime is emerging: cyber crime, causing more than $11 billion in losses. This paper asks how cyber crime is best deterred. It identifies five constraints on crime - legal sanctions, monetary perpetration cost, social norms, architecture, and physical risks - and explains how each of these constraints may be reduced by committing crime in cyberspace. Cyber crime requires fewer resources and less investment to cause a given level of harm, the law might want to use approaches that differ somewhat from those in real space. Criminal law must be concerned not only with punishing crime ex post, but with creating ex ante barriers to inexpensive ways of carrying out criminal activity. Some government barriers, however, will create dead-weight losses. The paper advocates the use of sentencing enhancements as tools that surgically target bad acts. Sentencing enhancements have received relatively little attention in the academic literature; this Article attempts to fill that gap. Cyberspace also adds additional parties to the traditional perpetrator-victim scenario of crime. Law should impose modest responsibilities on third parties because doing so promotes cost deterrence and capitalizes on what Reinier Kraakman has called
gatekeeper liability. Burden-shifting must not, however, sacrifice the value of interconnectivity and network effects [5].

This author has given brief idea about Cyber Space and Criminal Laws.

- **Commander Barbara Etters (Sep 2001) : THE FORENSIC CHALLENGES OF E-CRIME.** In this paper author wants to say that all law enforcement personnel have a basic understanding of search and seizure issues in relation to electronic evidence, also there is need for more advanced and ongoing training for those involved in the investigation of electronic crime and for specialist training for a cadre of expert staff involved in the forensic computing area. Investigators involved in the investigation of complex e-crime will require some essential forensic computing skills and knowledge. There is need of the greater use of outsourcing to the private sector. The recent report of the Parliamentary Joint Committee on the NCA has recommended that a national cyber-forensic facility be established. Many e-crimes of the future will be traditional crimes simply perpetrated via or facilitated through the use of ICT. Many offenders will leave their 'footprints' in cyberspace and new skills and techniques will be required to enable the criminal justice system to deal with the e-crime issue and prevent its occurrence [6].

The researcher used this paper for problems faced forensic Labs.

- **Susan W Brenner (April 2002) : University of Dayton School of Law,** in their paper entitled as “Cyber crime Investigation and Prosecution: The Role of Penal and Procedural Law ” they thought that, The development of the Internet and the proliferation of computer technology has created new opportunities for those who would engage in illegal activity. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal
activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity. Criminal activity poses challenges for legal systems, as well as for law enforcement. Legal tools include an arsenal of well-defined cyber crime offenses for use in prosecuting cyber criminals and procedural rules governing evidence-gathering and investigation. Cyber crime is often transnational in character; offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cyber crimes. The primary focus of the article is on penal laws simply because there tends to be more consistency in the way countries define criminal offenses than in the area of procedural law. In order to maintain the level of internal stability a nation must enjoy to survive and prosper, each country must have penal laws that protect the safety of individuals ("crimes against persons"), that preserve the integrity of at least certain types of property ("crimes against property"), that prohibit interference with the legal system ("crimes against the administration of justice"), and that proscribe attacks on the government ("crimes against the state"). It is, however, not possible to postulate the same level of generic consistency with regard to procedural law; although there are empirical constancies in the procedures law enforcement uses when investigating and prosecuting crimes, nations vary widely in the legal constraints they place on these processes [7].

This paper shows the relation between the procedural law and the Penal Acts.

- Devadatt Kamat(2002): Devadatt Kamat states in his research paper “Information Technology Act 2000 – A Contractual Perspective” that the validity and the formation of contracts form the kernel e-commerce
law. It shows the requirement for the e-commerce as well as the new terminology required to do e-commerce. Author has studied in detail regarding e-commerce that will guide me for further research in e-commerce. In the emerging global economy, e-commerce and e-business have increasingly become a necessary component of business strategy and a strong catalyst for economic development. The integration of information and communications technology (ICT) in business has revolutionized relationships within organizations and those between and among organizations and individuals. Specifically, the use of ICT in business has enhanced productivity, encouraged greater customer participation, and enabled mass customization, besides reducing costs.

With developments in the Internet and Web-based technologies, distinctions between traditional markets and the global electronic marketplace—such as business capital size, among others—are gradually being narrowed down. The name of the game is strategic positioning, the ability of a company to determine emerging opportunities and utilize the necessary human capital skills (such as intellectual resources) to make the most of these opportunities through an e-business strategy that is simple, workable and practicable within the context of a global information milieu and new economic environment. With its effect of leveling the playing field, e-commerce coupled with the appropriate strategy and policy approach enables small and medium scale enterprises to compete with large and capital-rich businesses.

On another plane, developing countries are given increased access to the global marketplace, where they compete with and complement the more developed economies. Most, if not all, developing countries are already participating in e-commerce, either as sellers or buyers. However, to facilitate e-commerce growth in these countries, the relatively underdeveloped information infrastructure must be improved [8].
This study helps the researcher about the relation between E-commerce and Cyber Space, Cyber Crime and Cyber Law.

- **Pradeep Tomar (2002):** “New Vision of Computer Forensic Science: Need of Cyber Crime Law” A Cyber space is a virtual space that has become as important as real space for business, education and politics. Computer Forensic which is new form of science allows for the evidence of cyber crime to be admissible in the court of law, when prosecuting the cyber criminal. In this paper, author firstly describes the computer forensic, cyber crimes, cyber laws of nation & technology challenges. Aim of this paper is to act as a catalyst to raise awareness regarding computer forensic which continues to grow as one of the most important branch of science and help in investigation of cyber crime which continues to grow as one of the most potent threats to the Internet and computer users of the cyber society of 21st century in India.

  Author James A. Lewis (December 2002) also mentioned how to access the rises of cyber terrorism, cyber war and other cyber threats. This paper looks at one set of issues – those related to cyber-terrorism and cyber attacks on critical infrastructure and their implications for national security. Author describes the four elements of a reassessment of the cyber threat.

  First, there is a need to put cyber-warfare and cyber-terrorism in the historical context of attacks against infrastructure. Second, there is a need to examine cyber attacks against a backdrop of routine infrastructure failures. There is extensive data on power outages, flight delays and communications disruptions that occur normally and the consequences of these routine failures can be used to gage the effect cyber-warfare and cyber-terrorism. Third, there is a need to measure the dependence of infrastructure on computer networks and the redundancy already present in these systems. Forth for the case of cyber-terrorism
there is use of cyber-weapons in the context of the political goals and motivations of terrorists, and whether cyber-weapons are likely to achieve these goals.

Author also mentioned how the infrastructure can be a target of attacks. Cyber attacks are likely to be single attacks. Once a hacker has gained access and the damage done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line [9].

The author gives importance of cyber forensic Lab, it helps in this research.

- **R. Benjamin, B. Gladman and B. Randell (2003)**: Protecting IT Systems from Cyber Crime Large-scale commercial, industrial and financial operations are becoming ever more interdependent, and ever more dependent on IT. At the same time, the rapidly growing interconnectivity of IT systems, and the convergence of their technology towards industry-standard hardware and software components and sub-systems, renders these IT systems increasingly vulnerable to malicious attack. This paper is aimed particularly at readers concerned with major systems employed in medium to large commercial or industrial enterprises. It examines the nature and significance of the various potential attacks, and surveys the defence options available. It concludes that IT owners need to think of the threat in more global terms, and to give a new focus and priority to their defence. Prompt action can ensure a major improvement in IT resilience at a modest marginal cost, both in terms of finance and in terms of normal IT operation[10].

Researcher found the number of techniques for protection to the systems.
• Talwant Singh (2004): According to Talwant Singh, Addl. Distt. & Sessions Judge, Delhi in his article “Cyber Law & Information Technology” states that what were the problem and technicality for the implementation of cyber law. This issue is a core part of our research. Actually the theme to do research in this area came to my mind after reading this article. This article shows that how difficult it is to implement the cyber law in practicality? Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe. Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law enforcement officers lacks the tools needed to tackle the problem; old laws didn’t quite fit the crimes being committed, new laws hadn’t quite caught up to the reality of what was happening, and there were very few court precedents to look to for guidance. Furthermore, a debate over privacy issues hampers the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust—between the two most important players in any effective fight against cyber crime: law enforcement agencies and computer professionals. Yet, close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe “place” for its users. Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT
personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal.

IT professionals need good definitions of cyber crime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offence. The first step in specifically defining individual cyber crimes is to sort all the acts that can be considered cyber crimes into organized categories [11].

This is relevant to present study undertaken by the researcher as it deals with cyber crime.

- Amit Nayak (2004): Understanding Cyber Crime Movements in Asia. The author focuses on the definition of cyber crime that IT professional should know when to report to police, also law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offence. The author says that first step in specifically defining individual cyber crimes is to sort all the acts that can be considered cyber crime into organized categories. Due to the global connectivity because of BPO, multimillion transactions can be conducted. The easy access to the internet and a booming market for related new communications devices have changed the way we spend, our leisure time and the way we do business. In today's world ways in which criminals commit crimes is also changing. Universal digital accessibility opens up new opportunities for the unscrupulous. Millions of dollars are lost to computer-savvy criminals by both businesses and consumers. Worse, computers and networks can be used to harass victims or set them up for violent attacks—even to coordinate and carry out terrorist activities that threaten us all. Unfortunately, in many cases law enforcement agencies have lagged behind these criminals, lacking
the technology and the trained personnel to address this new and growing threat, which has been aptly, termed cyber crime. The author says that many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were very few court precedents to look to for guidance. But even then close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users. The author, Quantify the Crisis as Cyber crime. It sounds exotic, the stuff of which futuristic science fiction novels are made. However, law enforcement officers, network administrators, and others who deal with crime and/or cyberspace are discovering that the future is now, and cyber crime is a big and growing problem.

He then has given various examples such as According to the Internet Fraud. Complaint Center (IFCC), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, between May 2000 and May 2001, its first year of operation, the IFCC Web site received 30,503 complaints of Internet fraud.

According to the Computer Security Institute's Computer Crime and Security Survey for 2001, conducted in conjunction with the FBI's Computer Intrusion Squad, 186 responding corporations and government agencies reported total financial losses of over US$3.5 million, due to primarily theft of proprietary information and financial fraud. According to the Cyber snitch Voluntary Online Crime Reporting System, Internet-related crimes range from desktop forgery to child pornography and include such potentially violent crimes as electronic stalking and terrorist threats. The author puts forth that almost anyone
has the potential to be affected by cyber crime, two groups of people must deal with this phenomenon on an ongoing basis: Information technology professionals, who are most often responsible for providing the first line of defense and for discovering cyber crime when it does occur and Law enforcement professionals, who are responsible for sorting through a bewildering array of legal, jurisdictional, and practical issues in their attempts to bring cyber criminals to justice. The author has given the definition of cyber crime by United Nations, Cyber crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime [12].

This paper helps in the research where crime can be done by the BPO employees at international level

- **Dr. Farooq Ahmad (2004)**: CYBER LAW IN INDIA (LAW ON INTERNET) book written by Dr. Farooq Ahmad, Reader, Department of Law, University of Kashmir, Srinagar-190006, is a good book to understand all tiny concepts required for this research. It has emphasized on implications of the Cyber Law in general. Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the present pace of life but at the same time also resulted in various threats to the consumers and other institutions for which it's proved to be most beneficial. Various criminals like hackers, crackers have been able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. and have been successful in gaining “unauthorised
access” to the user’s computer system and stolen useful data to gain huge profits from their accounts.

Intentional use of information technology by cyber terrorists for producing destructive and harmful effects to tangible and intangible property of others is called “cyber crime”. Cyber crime is clearly an international problem with no national boundaries. Hacking attacks can be launched from any corner of the world without any fear of being traced or prosecuted easily. Cyber terrorist can collapse the economic structure of a country from a place where the country might not have any arrangements like “extradition treaty” to deal with that criminal. The only safeguard would be better technology to combat. Such technology already evolved and known to the Hackers, but that still has threat of being taken over by the intellect computer criminals [13].

This book gives the fundamental information’s of Cyber Crime for the research work.

- N.S.Abouzakhar, A Gani and G Manson(Jan 2004) : Bayesian Learning Networks , Approach to Cyber crime Detection The author explained increase in the number of interconnected networks to the Internet has led to an increase in security threats and cyber crimes such as Distributed Denial of Service (DDoS) attacks. Any Internet based attack might take just a few minutes, hours, days, or even months before the attack takes place. This paper shows how probabilistically Bayesian network detects communication network attacks, allowing for generalization of Network Intrusion Detection Systems (NIDSs). Author used signature analysis or statistical anomaly detection approaches for detecting network attacks. In any statistical anomaly detection approach, the system requires the estimation of two quantities: the probability of detection (PD) and the probability of false alarm (PFA). This research paper proposes an innovative prediction...
approach for network intrusion detection. Author has also discussed concept of Bayesian learning networks model within the context of intrusion detection systems (IDSs), a model of Bayesian network for detecting network Distributed Denial of Service (DDoS) attacks, powerful learning methods to extract the variable nodes of Bayesian network directly from a dataset. Due to the decision tree's discretization, with attack type as the target node of the detector, all continuous contributed variables are automatically cut up into a number of intervals. Author used the lift curve performance results for a sample of DDoS attacks are given and, the results showed that Bayesian unsupervised learning models could reliably detect the majority of the existing attacks with minimum false alarm rates[14].

This paper concentrated on the attacks on internet use.

- **Kyung-shick Choi (April 2004):** Bridgewater State College, USA, in their paper entitled “Computer Crime Victimization and Integrated Theory: An Empirical Assessment”, as per their opinion they thought that, This study empirically assessed a computer-crime victimization model by applying Routine Activities Theory. Utilizing structural equation modeling facilitated the assessment of the new theoretical model by conveying an overall picture of the relationship among the causal factors in the proposed model. Society depends heavily on computer technology for almost everything in life. Today, computer criminals are using this increased dependency as a significant opportunity to engage in illicit or delinquent behaviors. It is almost impossible to have precise statistics on the number of computer crime and the monetary loss to victims because computer crimes are rarely detected by victims or reported to authorities. In addition, policing in cyberspace is very scarce. The purpose of this study is to estimate patterns of computer-crime victimization by applying routine activities
theory. The tenet of interest is how computer security, as an important capable guardian in cyberspace, plays a major role against computer-crime victimization.

Most people are confused about the difference between cyber-crime and computer crime. It is necessary to define the difference between cyber crime and computer crime. Casey defines cyber crime as "any crime that involves computers and networks, including crimes that do not rely heavily on computers". Thomas and Loader also note that cyber crime is "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks". Basically, cyber crimes cover wide categories of crime in cyberspace or on the World Wide Web including, "computer-assisted crimes" and "computer-focused crimes".

The computer crimes usually require more than a basic level of computer-operating skill for offenders to commit these crimes successfully against the victims. The focus of the proposed research is on individual victimization through computer crimes, particularly computer hacking, which can include the implantation of computer viruses. The number of individuals victimized by computer crimes has increased annually. Flanagan and McMenamin states that, computer crimes committed by the new generation of hackers, might cost cyber crime victims, as a collective, anywhere from $500 million to $5 billion an year. Unfortunately, the general population has still not recognized the overall seriousness of computer crime. In fact, many criticisms on computer crime related quantitative and qualitative research are driven from lack of "generalizable data" based on computer-crime incidents against private victims in quantitative research, and small sample sizes in qualitative research that may draw biased outcomes. The main contribution of this research is that it constitutes an inventive attempt to uncover computer crime victimization by integrating two criminological victimization theories with the empirical assessment of SEM. The
results of the empirical assessment demonstrate that online lifestyle and
digital guardianship are all important aspects of a model delineating
patterns of computer crime victimization [15].

The author Kyung-shick Chool throws light on the mentality of
offenders of Cyber Crime.

- **Brian Cashell, William D. Jackson, Mark Jickling, and Baird
Webel (April 2004):** The Economic Impact of Cyber-Attacks April 1,
2004  Brian Cashell, William D. Jackson, Mark Jickling, and Baird
Webel, Government and Finance Division, In this paper authors
describe the Information security – the safeguarding of computer
systems and the integrity, confidentiality, and availability of the data
they contain – has long been recognized as a critical national policy
issue. Author has explained the two current trends, first, the integration
of computers into more and more aspects of modem life continues.
Second, cyber-attacks, or breaches of information security, appear to be
increasing in frequency, and few observers are willing to ignore the
possibility that future attacks could have much more severe
consequences than what has been observed to date. Though cyber-
attacks have been relatively limited in scope Individual firms, may have
suffered significant losses as a result of past attacks. Author also
discussed the economic effect of cyber attacks on stock process. In
theory, the price of a company’s stock is primarily determined by the
present discounted value of the cash flows expected to result from that
firm’s output. That cash flow is what contributes to the wealth of the
stockholders, either in the form of dividends or in the expansion of the
firm’s stock of productive capital. Author said that any event that
changes investors’ expectations about that future stream of income is
likely to affect the price of the stock. Author has described the types of
attacks according to the business is affected. As long as any cyber-
attack is limited in scope and short-lived it is likely that macroeconomic consequences will be small. But the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs [16].

The above discussion helps to the researcher in financial Cyber Crimes.

- **Manish Lunker (2004):** Cyber Laws: A Global Perspective, In this, the author gives the introduction about how the information technology is encompassing all walks of life in the whole world. The information technology has made the transition from paper to paperless transaction possible. It also tells about the effective use of computers in storage of data politically, social, economic which brings immense benefit to the society.

  Due to the rapid growth in the internet, computer has emerged as a new form of crime especially internet related which virtually have no boundaries and may affect country across the globe. Thus, it is a necessity for legislation in all countries for the prevention of computer related crimes.

  The author tells cyber laws is required because crimes are considered as illegal, unethical or unauthorized behavior of people relating to the automatic processing and transmission of data, computer and networks.

Many countries such as USA, Austria, Denmark, France, Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore have come forward to meet challenges of cyber crime. Some of the major types of offences against which many countries across the globe have enacted various Acts (mostly at preliminary levels) are, Data spying, Forgery of prohibitive data, False entry in an authentic deed, False entry in permit,
licensure or passport, Unauthorized access with intention to commit
offences/ computer crimes, Knowingly access of computer without
authorization related to national defence or foreign relation, Intentional
access of computer without authorization to obtain financial
information, Unauthorized access of computer of a Govt. Dept. Or
agency etc [17].

This paper touches to all the countries those have enacted the Cyber
Law.

Adequacies of Computer-Related Criminal Legislation in the United
States, the United Kingdom and Singapore”. The author has
concentrated on cyber crime & its protection. Computer and Internet
usage is on the rise due to lower costs of computer ownership and
connectivity, as well as faster and easier accessibility. “Computer
Crime” encompasses crimes committed against the computer, the
materials contained therein such as software and data, and its uses as a
processing tool. These include hacking, denial of service attacks,
unauthorized use of services and cyber vandalism. “Cyber Crime”
describes criminal activities committed through the use of electronic
communications media. One of the greatest concerns is with regard to
cyber-fraud and identity theft through such methods as phishing,
pharming, spoofing and through the abuse of online surveillance
technology. Offences against the computer are relatively new as they
arise from and in relation to the digital age, which threatens the
functionality of the computer as an asset of a borderless information
society. New laws are required in order to nurture and protect an
orderly and vibrant digital environment. Offences through the use of
computers merely constitute new ways to commit traditional offences
using the electronic medium as a tool.
In this paper author has discussed about computer-related crime, in particular cyber crime such as phishing and its progeny, require a different solution due to the non-terrestrial and non-territorial nature of electronic transactions. In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized.

In order for there to be an effective global system to deal with the problem of computer-related crimes, there must be a multifaceted and multipronged approach using a combination of both legally coercive and non-legal measures [18].

This helps to the researcher to critically study what are the steps taken by the legislation in US, UK and Singapore.

- **Madhavi Divan(Oct 2004)**: The Research Article “The Right to Privacy In The Age of Information and Communications” is written by Madhavi Divan, Advocate, High Court, Mumbai. This article highlights on the development of the media in modern era with a special relevance to the evolution of the law of privacy. The media has made it possible to bring the private life of an individual into the public domain, thus exposing him to the risk of an invasion of his space and his privacy. This article relates us to the pornography crime mentioned in the Cyber Act 2000 and much more related crimes like credit card number etc. Since the turn of the century, we have experienced a sequence of revolutions in technology. The mechanization of agriculture reduced the percent of the U.S. population involved in feeding the nation from more than 50 percent to less than 3 percent. Machine tools capable of creating interchangeable parts from prehardened metal allowed the assembly of mechanical devices by relatively unskilled labor. The associated reduction in cost created markets that in turn created jobs and increased
prosperity. The ability to transmit electrical energy and the widespread use of internal combustion engines has had far-reaching impacts on our cities and on our goods and services distribution systems. Similarly, the advent of electronics has brought us communications and entertainment devices that have significantly improved the quality of our lives.

We have now entered the computing and information age. Although it is too soon to fully understand the implications, digital computing and fiber-optic communications are replacing mass and energy with information and computation. Companies are exploring ways to reduce the weight of automobiles by replacing individual wires with an electrical power bus. Digital signals are being used to inform light bulbs and other devices when to turn on or off. Engineers are exploring whether expensive mechanisms for accurately registering paper in high-speed copiers can be replaced with inexpensive mechanisms, compensating for the registration by rotating the image digitally. These and many other technologies will profoundly affect our lives by reducing costs, creating new services, and providing undreamed of access to information [19].

This study gave the information to the researcher about information and communication through Information Technology.

- Peter Grabosky (2005): “The Global and Regional Cyber Crime Problem”. This paper provides an overview of computer-related crime. Eleven varieties of crimes are considered: theft of services; communications in furtherance of criminal conspiracies; information piracy and forgery; the dissemination of offensive materials; cyber-stalking; extortion; electronic money laundering; electronic vandalism and terrorism; sales and investment fraud; illegal interception; and electronic funds transfer fraud. The most appropriate strategies for the control of computer-related crime entail a mixture of law enforcement,
technological and market-based solutions. It is argued that in some contexts, the market place may be able to provide more efficient solutions to the problems of computer-related crime than state interventions. This paper discusses current and emerging forms of computer-related illegality. It reviews eleven generic forms of illegality involving information systems as instruments or as targets of crime. It will also discuss issues arising from the global reach of information systems. It is trite to describe the ways in which computers have, figuratively speaking, made the world a smaller place. The corresponding potential for trans-jurisdictional offending will pose formidable challenges to law enforcement. For some crimes, this will necessitate a search for alternative solutions. Computer-related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control, and that security in cyberspace will depend on the efforts of a wide range of institutions. Trans-national crime of a more conventional nature has proved to be a very difficult challenge for law enforcement. Computer-related crime poses even greater challenges. There may be differences between jurisdictions about whether or not the activity in question has occurred at all, whether it is criminal, who has committed it, who should investigate it and who should adjudicate and punish it. Moreover, there is a fundamental tension between the deregulatory imperative which characterizes the world’s advanced economies and the desire to control some of the darker corners of cyberspace [20].

This helps to the researcher about comparison at Global with local problems.

- **Professor Soumyo D. Moitra (2006):** "Modeling Cyber crime for Internet Risk Management" Kolkata, India. In his published book author has concentrated on the cyber crime. Internet crime is considered
as a cyber crime. In this, cyber crime of basic modeling & its benefits are outlined. National policymakers & regional blocks have considered & to implement number of measures to control cyber crime. However, many policy making are based on media report, public reaction & ad-hoc data. Most of the surveys till date have serious methodological limitations. The author has focused on nature of cyber crime also. There are major gaps in our knowledge, such as the crime commission rate of malicious hackers, the relationship between cyber crime experienced at a site and the characteristics of that site or the detection and reporting rates of victim sites. Author has also discussed about secondary data. In recent years, a considerable number of reports have been published which present results of surveys or collected information on alleged cyber crimes. Internet risk management and the design of future surveys. It is important that models are developed first to guide the empirical research so that more meaningful survey instruments can be constructed. Then we shall be able to collect data that would provide accurate insights into the cyber crime process and yield results that would be useful to further our knowledge of cyber crime [23].

This is relevant to the present study undertaken by the researcher as it deals with Cyber Crime.

- **Florence Tushabe, and Venansius Baryamureeba (2007) : “Cyber Crime in Uganda: Myth or Reality?”** The author has focused on cyber crimes in Uganda. There is a general feeling that Internet crime is an advanced type of crime that has not yet infiltrated developing countries like Uganda. The author conducted an independent research to ascertain whether cyber crimes have affected people in Uganda and if so, to discover where they are reported? Internet users in Uganda have not been victims or perpetrators of Internet crimes? Informal and scanty reports about computer crime in Africa and in Uganda particularly result in a misconception that those crimes do not feature there. They
include crimes like cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, Internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more. Authors study has revealed that cyber crime is silent but common even in the developing countries like Uganda. As much as 90% of Internet users in Uganda have suffered losses caused by Internet crimes. It is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise [22].

This is relevant to the present study about what steps were taken outside India.

• Rohas Nagpal (2008): CYBER TERRORISM IN THE CONTEXT OF GLOBALIZATION "Globalization and Human Rights", The paper focuses and examines on the tools and methodologies of cyber terrorism such as viruses, worms, Trojans, denial of service attacks and cryptography. It also focuses on measures both legislative and reactive measures taken by various countries to get rid of cyber crime in general and cyber terrorism in particular. The paper gives some examples of cyber terrorism in the recent past. According to the author, cyber terrorism is the use of disruptive activities and a threat in cyber space. The author has given examples like hackers have taken down national defense system, taken control of huge dam, shut down large segments of Americas power grid, disrupted troop deployments during the gulf War etc [21].
The author gives the relation of Human Rights with Cyber laws.

REFERENCES:

1. I.G. Rathinasabapathy, Cyber Crimes and Information Frauds: EMERGING CHALLENGES FOR PROFESSIONALS, 1991-[Book]


6. Commander Barbara Etters, THE FORENSIC CHALLENGES OF E-CRIME, Australasian Centre for Policing Research, PO Box 370, Marden, South Australia, 5070, AUSTRALIA, Sep 2001-[Research Paper]
7. Susan W Brenner, University of Dayton School of Law, "Cyber crime Investigation and Prosecution, April 2002-[Research Paper]


14. Dr. Farooq Ahmad, CYBER LAW IN INDIA (LAW ON INTERNET) book written by Dr. Farooq Ahmad, Reader, Department of Law, University of Kashmir, Srinagar-190006, 2004-[Research Paper]
15. N.S. Abouzakhar, A Gani and G Manson, Bayesian Learning Networks, Jan 2004-[Research Paper]


23. Professor Soumyo D. Moitra,"Modelling Cybercrime for Internet Risk Management" Kolkata, India, Jan 2006-[Book]