CHAPTER – I
INTRODUCTION

In today's world there is no one who is not touched by the Information Technology (IT)\(^1\) revolution at least remotely. The two technological marvels, i.e. computer and the networks have changed the way we live. There is hardly any facet of our lives that is not touched by the IT revolution. It covers almost all the manufacturing, marketing and services sectors. Communications, banking, railways, air travel, education, agriculture, medical, administration of Justice—these are only the glimpse of various sectors that are deeply affected by the advancements in the I.T.

COMPUTER

Computer An amazing machine! We are living in the computer age today and most of our day-to-day activities cannot be accomplished without using computers. Sometimes knowingly and sometimes unknowingly we use computers. Whether we have to withdraw money from the ATM, publish a newsletter, drive a motorbike, design a building or even a new dress, go to a grocery shop and buy from cookies to tyres for our car—all involve computer in one way or the other.

We are breathing in the computer-age and gradually computer has become such a dire necessity of life that it is difficult to imagine life without it. For most of the people, computer\(^2\) is a machine used for calculations or computation, but

---

1 Information Technology is concerned with managing processing of information especially within a large organization or company. The Penguin Dictionary of Computers defines the term "Information Technology" as a portmanteau phrase to cover all aspects of the art or science of processing of data to produce information. It includes computer software, hardware, programs and data bases, use of Internal and allied equipment that are used to store, process and transmit information across network of computers, Encyclopedia of IT Law, Sweet and Maxwell, Vol.II, 2001, p.201; http://www.webopedia.com; http://www.nsla.org/shot/toolkit/tiol.html; http://www.mcrel.org/products/teh/technology/impact.asp; http://mt.sopris.net/mpe-impactoftechnologyofsociety.

2 Section 2(1) (i) of IT (Amendment) Act, 2008 the term 'computer' means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
actually, it is much more than that. Precisely, "Computer is an electronic device for performing arithmetic and logical operations", or "computer is a device or flexible machine to process data and converts it into information."  

Today's computers are more powerful, smaller, cheaper, and more user friendly. The increased use of computers has been mainly due to the advent of the Internet.

INTERNET

The most recent and probably the greatest development in the whole history of information technology has come as a result of fast development internet and cyberspace. The internet today has changed the world in many ways. Internet has also made this world a virtual sleepless global marketplace. These technologies have created many new businesses and most importantly they have changed the way most businesses are conducted. The new businesses and new ways of conducting them, which are collectively called 'Internet commerce' or 'e-commerce', is on the growth path. Internet has removed the time and space restrictions for carrying out business and commercial activities. Undoubtedly, computers and IT have brought in unprecedented benefits to the individuals, organizations and society at large.

The Internet is a giant network of individual computers that are interconnected through a complicated structure of servers. Internet is a network of large number of computers, local computer systems hooked to regional systems hooked to national or international high capacity 'back bone' system. Each link, or node, in this web is a computer or computer site, all connected together by a variety of

connections. Each computer in the network communicates with the others by employing machine—language conventions known as the IP, or Internet Protocols. Indeed, it is these protocols that define the network; the network in which computers talk to one another using IP is the Internet.¹

In this modern information age the information is power and the Internet and cyber space allows free flow of information beyond all manmade boundaries.

The Internet users has significantly increased over the past few years.² From 2000 to 2009, the Internet has expanded at an average rate of 399.3 percent on a global level, and currently an estimated 1.8 billion people are “on the Net”. The increase in Asia has been 568.8 percent and in Africa 1809.8 percent.³

### WORLD INTERNET USAGE AND POPULATION STATISTICS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>991,002,342</td>
<td>4,514,400</td>
<td>86,217,900</td>
<td>8.7%</td>
<td>1,809.8%</td>
<td>4.8%</td>
</tr>
<tr>
<td>Asia</td>
<td>3,808,070,503</td>
<td>114,304,000</td>
<td>764,435,900</td>
<td>20.1%</td>
<td>568.8%</td>
<td>42.4%</td>
</tr>
<tr>
<td>Europe</td>
<td>803,850,858</td>
<td>105,096,093</td>
<td>425,773,571</td>
<td>53.0%</td>
<td>305.1%</td>
<td>23.6%</td>
</tr>
<tr>
<td>Middle East</td>
<td>202,687,005</td>
<td>3,284,800</td>
<td>58,309,546</td>
<td>28.8%</td>
<td>1,675.1%</td>
<td>3.2%</td>
</tr>
<tr>
<td>North America</td>
<td>340,831,831</td>
<td>108,096,800</td>
<td>259,561,000</td>
<td>76.2%</td>
<td>140.1%</td>
<td>14.4%</td>
</tr>
<tr>
<td>Latin America/Caribbean</td>
<td>586,662,468</td>
<td>18,068,919</td>
<td>186,922,050</td>
<td>31.9%</td>
<td>934.5%</td>
<td>10.4%</td>
</tr>
<tr>
<td>Oceania/Australia</td>
<td>34,700,201</td>
<td>7,620,480</td>
<td>21,110,490</td>
<td>60.8%</td>
<td>177.0%</td>
<td>1.2%</td>
</tr>
<tr>
<td>WORLD TOTAL</td>
<td>6,767,805,208</td>
<td>360,985,492</td>
<td>1,802,330,457</td>
<td>26.6%</td>
<td>399.3%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

NOTES: (1) Internet Usage and World Population Statistics are for December 31, 2009.

² Kaur Harpreet, "Cyber Law an Overview" Nyaya Deep, p. 83.
Internet Users in the World by Geographic Regions - 2009

<table>
<thead>
<tr>
<th>Region</th>
<th>Millions of Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia</td>
<td>764.4</td>
</tr>
<tr>
<td>Europe</td>
<td>425.8</td>
</tr>
<tr>
<td>North America</td>
<td>259.6</td>
</tr>
<tr>
<td>Latin America / Caribbean</td>
<td>186.9</td>
</tr>
<tr>
<td>Africa</td>
<td>86.2</td>
</tr>
<tr>
<td>Middle East</td>
<td>58.3</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>21.1</td>
</tr>
</tbody>
</table>

World Internet Penetration Rates by Geographic Regions - 2009

<table>
<thead>
<tr>
<th>Region</th>
<th>Penetration Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>76.2%</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>60.8%</td>
</tr>
<tr>
<td>Europe</td>
<td>53.0%</td>
</tr>
<tr>
<td>Latin America / Caribbean</td>
<td>31.9%</td>
</tr>
<tr>
<td>Middle East</td>
<td>28.8%</td>
</tr>
<tr>
<td>Asia</td>
<td>20.1%</td>
</tr>
<tr>
<td>Africa</td>
<td>8.7%</td>
</tr>
<tr>
<td>World, Avg.</td>
<td>26.6%</td>
</tr>
</tbody>
</table>
World Internet Users Distribution
by World Regions - 2009

INTERNET USERS AND POPULATION STATISTICS FOR ASIA

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Only</td>
<td>3,808,070,503</td>
<td>56.3 %</td>
<td>764,435,900</td>
<td>20.1 %</td>
<td>568.8 %</td>
<td>42.4 %</td>
</tr>
<tr>
<td>Rest of the World</td>
<td>2,959,734,705</td>
<td>43.7 %</td>
<td>1,037,894,557</td>
<td>35.1 %</td>
<td>320.7 %</td>
<td>57.6 %</td>
</tr>
<tr>
<td>WORLD TOTAL</td>
<td>6,767,805,208</td>
<td>100.0 %</td>
<td>1,802,330,457</td>
<td>26.6 %</td>
<td>399.3 %</td>
<td>100.0 %</td>
</tr>
</tbody>
</table>

NOTES: (1) Asiatic Internet Usage and Population Statistics were updated for December 31, 2009.
Internet Penetration in Asia
2009 (year-end)

Asia
World Average
Rest of World

Penetration (% Population)

Internet in Asia - 2009
Top 10 Countries

China
Japan
India
Korea, South
Indonesia
Philippines
Vietnam
Pakistan
Malaysia
Thailand

Millions of Users

0 50 100 150 200 250 300 350 400 450

384.0

96.0

81.0

37.5

30.0

24.0

22.8

18.5

16.9

16.1
The word 'Cyber Space'\(^1\) was never known to the world until 1984. The word 'Cyber space' (from Cybernetics and space) was coined by science fiction novelist and seminal cyberpunk\(^2\) author William Gibson in his 1982 story "Burning Chrome" and popularized by his 1984 novel "Neuromancer."\(^3\) According to Gibson, 'Cyber space' refers to that imaginary space which is created by computers when they communicate. Cyber space is thus an abstract concept that represents an area where a kind of activity takes place in which the computers connected through a network are engaged. It is that invisible realm in which one particular computer is linked to other computers in the world, and retrieving on

\(^{1}\) The word cyber space refer to a near-future computer network where users mentally travel through matrices of data. The term is now used to describe the Internet and the other computer networks. A popular name for the internet and allied electronic resources (from cybernetics the science of communication and control theory). Popular term now associated with the internet, which describes the national information 'space' that is created across computer networks; Agarwala Deeksha, "Glossary of IT Terms", Mcmillan India Ltd., New Delhi, Ed. 2003, p.83.


sending almost any information anywhere in more than 150 countries cheaply, quickly and reliably. Cyber space is real time, online communication through high speed data links that crisscross the globe. It is often referred to as the 'Information Highway'.

The Shorter Oxford English Dictionary explain the expression ‘cyber space’ as notional environment within which electronic communication occurs, especially when represented as the inside of a computer system; space perceived as such by an observer but generated by a computer system and having no real existence; the space of virtual reality.

The term 'cyber' derives it origin from 'cybernetics' which means science of systems of control and communications in living organism and machines. The word 'cyber', apparently referring to the science of cybernetics, was well-chosen for this purpose, as it derives from the Greek verb 'Kubernao', which means 'to steer' and which is the root of our present word 'to govern'. It connotes both the idea of navigation through a space of electronic data, and of control which is achieved by manipulation those data. For example, in one of his novels William Gibson describes how someone, by entering cyber space, could steer computer-controlled helicopters to a different target. Gibson's cyber space is thus not a space of passive data, such as a library: its communication channels connect to the real world, and allow cyberspace navigators to interact with that world. Cybernetics defines itself as a science of information and communication, and cyberspace’s substrate is precisely the joint network of all existing communication channels and information stores connecting people and machines. The word

3 Ibid.
4 The term ‘cybernetics’ was coined by Norbert Winner in the 1948s, based on a Greek word meaning ‘steersman’, David A. Mindell, “Cybernetics”, p.3, http://web.mit.edu/esd.83/www/notebook/Cybernetics.PDF; Although the term has tended to fall into disuse with the expansion of the computer field, cybernetics is essentially a broad-based discipline which includes information, message, and noise theories, and can reconcile the work of neurophysiologists, psychologists, and computer engineers, David Crystal, “The New Pengium Encyclopedia”, Pengium Books, New Delhi, Ed. 2002, p. 414.
'space', on the other hand, connotes several aspects. First, a space has a virtually infinite extension, including so many things that they can never be grasped all at once. This is a good description of the already existing collections of electronic data, on e.g. the Internet. Second, space connotes the idea of free movement, of being able to visit a variety of states or places. Third, a space has some kind of a geometry, implying concepts such as distance, direction and dimension.\textsuperscript{1} Cyber space is one of the great legal frontiers of our time.\textsuperscript{2}

**CYBER CRIME**

It is the history of all technological advances that alongwith the improvements they bring about in the human life, they also bring some bad effects. If we look into some of the technological revolutions that changed the human life like, the automobile, the telegraph, and the telephone, for example— they all have brought dramatic improvements for society, but have also created new opportunities for wrongdoing.\textsuperscript{3} ‘The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors—such as education, research, commerce, entertainment, and discourse on public affairs—in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts.’

The Information Technology revolution is unparalleled. There is no aspect of life that the information technology is not affecting at least indirectly. Rapid growth of technology, especially the seemingly limitless spread of Internet is changing the way we all live; and changing the way the criminals operate. The Internet provides many an advantage to the criminals to spread their activities. Enhancement of anonymity afforded by the communication modes like e-mail,

\begin{itemize}
\item \textsuperscript{1} Heylighen, "Cyber space", \url{http://pespmc1.vub.ac.be/cyberspace.html}
\item \textsuperscript{2} Francesca Bosco, "The negative impact of cybercrime on the financial sector and the economy", 5 May 2010, p.2, \url{http://www.ictparliament.org/parliamentaryforum2010/contribution/Bosco_Unicri_3PF.pdf}.
\item \textsuperscript{3} The Electronic Frontier: The Challenge of Unlawful Conduct Involving the use of the Internet, A Report of the US President's Working Group on Unlawful Conduct on the Internet, \url{http://www.cybercrime.gov}.
\end{itemize}
chat rooms, etc in the Internet allows criminals to operate freely. The organized criminal gangs also advantageously use this aspect in coordinating and widening their activities even beyond national borders. Secondly, the criminals all over the world is experimenting as to ways in which traditional crimes can be committed with the help of information technology. Another influence of information technology on criminality is in the way it is shrinking the whole world into a global village. This development not only brings the normal people together but also brings criminals world over together in their activities. Finally, increasing automation of our activities and convergence of telecommunication and information technologies are making all the aspects of human life susceptible to cyber criminals.

The word ‘cyber’ and its relative “.com” are probably the most fashionable words in the entire vista of the English vocabulary today. In the information age the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of transnational crimes known as 'cyber crimes'. Cyber crimes have virtually no boundaries and may affect every country in the world. Cyber crimes are a very serious threat for the times to come and pose one of the most difficult challenges before the law enforcement machinery. Most cyber crimes do not involve violence but rather greed, pride, or play on some character weakness of the victims. It is difficult to identify the culprit, as the Net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber crimes are considered as 'white-collar crimes'. To understand cybercrime as a significantly new phenomenon, with potentially profound new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently effecting countries worldwide.

---

2 Crimes committed by business people, professionals, and politicians in the course of their occupation as known as 'white-collar' crimes.
It today's environments, most businesses and government processes could not survive without the computer-especially email or totally web-based businesses. Without computers, entire businesses and government operations would almost cease to function. Criminals use computers to support their illegal operations. Computer crimes and frauds are increasing. They will no doubt continue to increase as more computers are networked internationally, thus giving global access to computer criminals.1

Cyber space has no specific jurisdiction; therefore, criminals can commit crime from any location through computer in the world leaving no evidence to control. Protection of information is keeping symbolic representation from harm or in other words it is preventing harm caused by symbolic representations. It is a form of self-defence in cyberspace which cannot be left to others. It is very difficult to control cyber crime because (i) criminals are well aware about security and preventive measures; (ii) they hardly leave any evidence; (iii) lack of adequate legislation to control them; (iv) lack of awareness among users; (v) lack of defined jurisdiction in cyberspace, cybercrimes took international shape; (vi) traditional laws are not adequate and present information technology law is not enough to prevent and control cyber crimes; (vii) cyber crimes are not adequately defined and scope is not specified; (viii) lack of expert law enforcing agencies with infrastructural support; and (ix) lack of expert judicial system with infrastructure.2

Cyber crime is a threat to national and international socio-economic, political and security system.3 The increasing use of the Internet has also led to an increase in cyber crime.4 When internet was developed, its founding fathers did not probably imagine that internet could also be misused for criminal activities. However, today there are many disturbing things happening in cyber space,

especially the cyber crimes. It will not be out of place to mention here that cyber crime has acquired international dimensions and that today the cyber criminals can move at the speed of light on a highway on which there are no traffic signals, no constables and no custom or immigration authorities to check them for anything.

Traditionally the duration of criminal acts is measured in minutes, hours, days, weeks, months and years. Thus automated crime must be considered in terms of a computer time scale of milliseconds, microseconds and nanoseconds because of the speed of execution of instructions in computers. Computer crime may involve computers not only actively but also passively. If a computer is stolen in a simple theft where, based on all circumstances, it could have been a washing machine or milling machine, a knowledge of computer technology is not necessary and it would not be a computer crime. However, if knowledge of computer technology is necessary to determine the value of the article taken, the nature of possible damage done in the taking or the intended use by the thief, then the thief would be a computer crime. Cyber crimes are not any new crimes. They are just the traditional crimes committed through computer and internet.

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and various services.

The term 'cyber' means "a prefix overused to indicate a connection to computers, networks, technology or futurism."

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 is defined as "a legal wrong that can be followed by criminal proceedings which may result into punishment." A crime may be said to by any conduct accompanied by act or

omission prohibited by law and consequential breach of which is visited by penal consequences.¹

Cyber crime is a broad and generic term that refers to crimes committed using computers and the internet.² Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.³ In other words computer crimes are those that are committed either on a computer system or with the aid of such a system.⁴

The IT Encyclopedia .com define the word ‘cyber crime’ as “criminal activities in cyber space”.⁵ Cyber crime has been defined as the act of creating, distributing, altering, stealing, misusing and destroying information thorough the computer manipulation of cyberspace; without the use of physical force and against the will or the interests of the victim. As a concept, information can be anything from electronic money, to government secrets, and the victim can be an individual, a corporate person, or as criminal law is defined the state and society as a whole.⁶

‘Cyber crime’ or ‘Computer Crime’ generally speaking computer crime is a form of white-collar crime, meaning thereby, that it is usually committed by the individuals/professionals or organizations during the course of their occupation/profession etc. Nevertheless, some of the commonly spelt out definitions of ‘cyber crime’ are:

---
A criminal activity that involves unlawful access to, or utilization of, computer systems.

Any illegal action in which a computer is used as a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the functions of a computer.

Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

Any violation of the law in which a computer is the target of or the mean for committing crime.¹

The Organization for Economic and Cultural Development (OECD) however, has adopted the following definition as the working definition for computer-related crime or computer crime “computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data”.

Cyber crime means any activity which involves the unauthorized and unlawful access to or utilization of computer system or networks in order to tamper with the data or to intentionally transact anything illegal with the help of computers and the Internet can broadly be called as ‘cyber crime’.

Cyber crime means “when a computer is used in the commission of such crime or computer technology is responsible for the wrongful gain or wrongful loss of a party or there has been an illegal use of computers in the processing and transmission of data.”²

To conclude, it may be stated that various terms and definitions that came into scene have only helped in obfuscating the concept further. What exactly is a computer crime or cybercrime? We can safely state that these

terms are not amenable to a precise definition. It could simply be a technological rendition of a traditional crime or it could be an innovative crime that came up due to prevalence of computers and networks. That is why most of the world legislations fighting cybercrime do not attempt a definition of the term.

Cyber crimes-harmful acts committed from or against a computer or network-differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

ELEMENTS OF CYBER CRIME AND CRIMINAL LIABILITY

From the definition of crime it is clear that there are two elements of crime one is mens rea and another is actus reus with certain exceptions e.g., in conspiracy only mens rea is enough for imposing criminal liability. In crime against State e.g. false evidence, counterfeiting coin, white collar crime, etc. only actus reus are sufficient to impose criminal liability. The general principle of criminal law is that no person is to be convicted of a crime unless it is proved beyond reasonable doubt by the prosecution that his conduct (act or omission) is prohibited by criminal law and he is liable for the same and also that he had a defined state of mind in relation to the crime commission. In other words actus reus unaccompanied with mens rea is not a crime.

\[
\text{Actus reus} + \text{Mens rea} = \text{Crime}
\]

\[
\text{Actus reus} + \text{No Mens rea} = \text{No Crime}
\]

\[
\text{No Actus reus} + \text{Mens rea} = \text{No Crime}
\]

This is the general principle that crime consists of two essential elements. There are five essential requirements for imposing criminal liability. These are: (1) human conduct; (2) circumstances; (3) consequences or result; (4) voluntariness; (5) foreseen or forcibility of result of his conduct in a circumstance which has causation of crime and there must be chain of causation and probable or natural

---

consequence. Fifth one i.e., forcibility represent mens rea and other four requirements represent actus reus. So, it is not permissible and unjustified for the State to impose punishment where any one of the elements is absent; except exceptional cases. 'Actus reus' is 'human conduct' or act which includes omission and under s. 33 of the Indian Penal Code 1860, act includes omission.

A well-known definition of actus reus is "as such result of human conduct as the law seeks to prevent".1 In rape the absence of consent on the part of the prosecutrix is an essential constituent of the actus reus. If this absence of consent is not proved by the prosecution then actus reus of the accused will also not prove and here the prosecution will fail. In this sense we can say sometimes mens rea is also the part of actus reus.

In case of cyber crime it is very difficult to prove both elements of crime. Actus reus of cyber crime is very dynamic and varied. For example when with a keyboard and mouse one start functioning with computer, when one is attempting to access information on others computer without the consent or approval of the authorized person, when is one attempting for hacking, flowing viruses, to commit cyber terrorism and actually caused those acts these are human conduct or actus reus in cyberspace which law seeks to prevent. These are again actus reus of cyber crime.

Mens rea is another essential element of cyber crime. 12th century only for actus reus a roan could be held liable for any injury without proof of mens rea or blameworthy state of mind. In modern Common Law this concept has been changed and now guilty mind or blameworthy state of mind is the essential element for crime commission and imposition of penalty.2 Words such as, recklessness, negligence, intention, knowingly, dishonestly, fraudulently etc. represents mens rea.3 Mens rea is not used and defined in the Indian Penal Code 1860 which is one of the major criminal laws in India. However, Indian Penal

---

Code defines dishonestly, fraudulently etc. There must be on the part of the cyber criminal foresight or *meres rea* to commit crime. For example, while committing hacking, hackers have knowledge or intention of unauthorized access and thereby commission of crimes.

When any person knowing or intentionally accesses without the permission of the authority (1) any information, computer, computer system or network therein and alters, damages, deletes, destroys or uses those devises or executes any unlawful plan, defrauds or wrongfully controls for financial gain and causes wrongful loss by this way; (2) alters or copies any supporting documentation external or internal to it or adds, alters, damages, deletes, destroys any database software, programmes which reside or exist internal or external to a computer, computer system or computer network; or (3) disrupts or causes the disruption of computer services or denies or causes the denial of services to an authorized user of a computer network, computer system; or (4) provides or assists in providing a means of accessing a computer, computer system or computer network; or (5) with the intent to defraud or to abets to false representation, false statement; or (6) to install or tamper others computers, computer system, computer network; or (7) to flow virus or objectionable information e.g., pornography; are cyber crimes. Knowingly or intentionally both the words represents *mens rea* in cyber crime and other conduct are *actus reus*.

The cyber jurisprudence is still in the process of evolution. It mainly aims at:

1. An integration of various technologies and legal aspects of information technology.
2. An examination into the nature of various cyber laws so far having been passed including especially their working pattern with particular reference to their societal impact.
3. An examination into the possibility of enacting more and more relevant cyber legislation, filling in the gaps appearing in working of the cyber laws already enacted.
4. Relative freshness of the cyber society where the fundamental principles of cyber jurisprudence are yet to be developed.
5. The emergence of a field of study for a new crop of professionals who may be called as Techno- Legal Experts.
Exposing a technology student to law and vice-versa; as neither the technologist nor the lawyers are alone competent to understand the niche aspects of cyber laws.

Cyber law is a relevant knowledge for all of us living in a society with increasing use of computer and Internet. It is the fundamental law of the cyber space. Software professionals who actually create cyber space and who spend for most part of their day in it must absorb emerging salient features of cyber laws. Similarly, corporate executives who own and manage cyber space properties also need to be well conversant with cyber laws so that they would be able to discharge their functions properly.

Knowledge of cyber laws are therefore essential for everyone who directly or indirectly interacts with internet based services or with other proprietary networks of banks, stock brokers, intra-company and inter-company information exchange systems etc. The day has now arrived where internet and computer networks have become as much a part of our society as the public road, gas, reservation or electricity etc while some of us may personally not like to use this gadgets at present or use it only for restricted purposes, the environment may force encounters with cyber world.

REVIEW OF LITERATURE

The literature resource for analysis is available in the form of number of books, newspaper, magazines, internet sites, journals, articles, conventions and relevant laws in different countries. The literature relating to the nature and type of cyber crime and laws relating to combat cyber crime, international conventions and conferences affecting the national scenario have been studied in detail. The internet had a substantial effect to studying international scenario as well as definitions of different words and news items, without which the research would have been much more difficult. All sources of information, digital or otherwise, have been cited in footnotes to the main text and these may serve as useful tool to guide those desiring to undertake in depth research in any of the areas that the work contains. One word of caution though: websites and URLs being rather transient in nature, sometimes links might have lapsed, the footnotes only tell of those sites that existed at the time of writing along with the date when they were accessed.
Amita Verma have submitted and awarded the Ph.D. Thesis in the year 2004. The subject of this Ph.D. was *Cyber Crimes: An Analytical Study of International and National legal regimes*. In that Ph.D. the candidate has put up in XI following chapters.

Chapter 1 : Introduction
Chapter 2 : Cyber space : the conceptual framework : Globalisation and information technology; Computer, Internet and its concept; cyber space
Chapter 3 : Concept of Cyber Crime, Challenges of Cyber Crime.
Chapter 4,5,6 & 7: Different types of Cyber Crimes.
Chapter 8 : International Laws related to Cyber Crimes
Chapter 9 : Judicial response
Chapter 10 : Empirical and evaluative critique
Chapter 11 : Conclusion and Suggestions

In that Ph.D. Thesis candidate give provisions of the Information Technology Act, 2000 but she did not submit the provision of IT (Amendment) Act 2008 and she also have not given provision of Prevention and Investigation of Cyber Crime. The second thing is that candidate Amita Verma has not put up also the International Initiative to combat Cyber Crime.

So the above important reasons I am in the position to did correct and up to date knowledge and information regarding Cyber Crimes in the current scenario of the changing and challenging world.

David S. Wall's book *Cybercrime: The Transformation of Crime in the Information Age*¹ is an exploration of the transformations that have taken place in criminal activity and its regulation as a result of networked technologies.

Wall acknowledges in the preface that the task of describing cybercrime is hard as the subject matter changes rapidly. Nevertheless, three years after Wall finished his work it is still in many ways current. The fast pace of evolving cyber crime is not the only challenge researchers face. As Wall points out, discussion around cyber crime has been dominated by media and politicians who often act out of fear and without real knowledge of the nature and scale of the problem. This

---

has often lead to the introduction of new legislation which has tried to satisfy the interests of corporate and State, while at the same time discussion of the principles of liberty and freedom of expression has been dampened.

David Wall’s work provides two excellent distinctions. Firstly, Wall distinguishes the generations of cyber crimes. First generation cyber crime used computers for criminal activity, whereas second generation cyber crime is committed in networks. The emerging third generation of cyber crime is automated and mediated by Internet technology.

Secondly, Wall groups cyber crime into three groups: Offences related to the integrity of the computer system, offences assisted by computers and offences which focus upon the content of computers.

These distinctions make the cyber crime phenomenon easier to grasp. It is easier to study and fight crimes that are more narrowly defined. Wall’s criminals are crackers, spammers and script kiddies who spread malicious software and try to scam our money and hijack our computers. Nevertheless, many European countries have criminalized peer-to-peer file sharing which turns tens of millions of teenagers into cyber criminals. The everyday cyber crimes where the criminals are not the Chinese mafia or nasty black hat hackers is something that Wall ignores. However, Wall’s book might not be the right forum to examine the question.

Cybercrime is a well researched, thoughtful and up-to-date examination of the reasons why cyber crime flourishes. It describes how we have ended up in the current situation and how we could study and fight cyber criminals.

*Pavan Duggal book Cyber law: The Indian Perspective*¹ is hefty book provides a comprehensive overview of the cyber law scenario in India, provides recommendations for upgrading the current cyber law acts, and contextualizes these developments with respect to actual reported cases of cyber law in India.

The material is well researched and clearly presented in 36 chapters and covers many areas in details e.g. a detailed analysis of the Information Technology Act, 2000, the recent cyber crimes cases in India, need for taking the required measures, emerging cyber law practices, issues pertaining to terrorism and cyber

---

¹ Ed.2000, Saakshar Law Publications, Delhi
of cyber harassment and spamming, cyber frauds, Indian consumers and cyber space.

The book also highlights the grey areas in cyber legislation. Interestingly, this book illustrates cyber law cases that indicate the ignorance of police officials. The author, through this book, presses urgently for the need to train police officials to tackle cyber offences with better awareness and knowledge.

*Dr. Marjie T. Britz* book *Computer Forensics and Cyber Crime*¹ fully defines computer-related crime and the legal issues involved in its investigation. Re-organized with different chapter headings for better understanding of the subject, it provides a framework for the development of a computer crime unit. Updated with new information on technology, this book is the only comprehensive examination of computer-related crime and its investigation on the market. It includes an exhaustive discussion of legal and social issues, fully defines computer crime, and provides specific examples of criminal activities involving computers, while discussing the phenomenon in the context of the criminal justice system. Computer Forensics and Cyber Crime is provides a comprehensive analysis of current case law, constitutional challenges, and government legislation. New to this edition is a chapter on Organized Crime & Terrorism and how it relates to computer related crime as well as more comprehensive information on Processing Evidence and Report Preparation.

*Jane book Cyber Crime*² attempts to provide a greater understanding and awareness of the world of information insecurity and the impending natures of cyber-threats through the identification of the problem, potential solutions, and the development of an action plan. The book attempts to highlight the techniques that cyber-criminals are likely to use as their primary means of communication in the current state of the technology, such as untraceable emails, encryption, and digital compression. The book is divided into four primary sections. First, the task of identifying how vulnerable information systems and networks are in the world is addressed. Secondly, the potential solutions that can help prevent breakdowns, and how speedily they can be actually put into place are presented. Third, the missing

---

¹ Ed. 2008, Publisher: Prentice Hall
² Ed. 2005

20 (i)
elements in any action plan are highlighted and the development of effective ICT security strategies is discussed. The fourth and final section sets out specific recommendations for information security. The book is directed towards decision makers in both the private and public sector in hopes of the drafting and adopting of a comprehensive Law of Cyber-Space.

J. A. Hitchcock book *Net Crimes & Misdemeanors: Outmaneuvering the Spammers, Swindlers, and Stalkers Who Are Targeting You Online*\(^1\) the author uses real stories to show what has happened to people in the past and then analyzes what can be done about it. She provides many Web resources for obtaining further information or getting help. The book covers such situations as cyberstalking, spam, urban legends and hoaxes, online shopping and auctions, and chats and offers several chapters that provide advice on how to keep you, your children, and your computer safe.

Many of the perpetrators of online trouble have some real-world connection with their victims in cyberspace—an ex-worker, ex-spouse, disgruntled employee, or unhappy customer—but cyberspace provides an easier outlet for their malicious intentions than the physical world. From the examples in the book, it is obvious the current legislation and police activities are struggling to catch up with these new-style crimes. Hence, this book is an important resource for those seeking help. What would you do if you were suddenly receiving thousands of spam e-mails a day? What if personal information about you appeared on a Web site? Read this book and find out how to handle these situations.

The author has written the book at a level that even a fairly novice user can understand, while still being useful to the more experienced. She takes the time to explain exactly what is happening in the various situations with technical explanations of how to track through e-mail headers, cookie files, and cache files. This is a must-read book for anyone using the Internet. Being aware of what can happen is the first step in preventing these crimes, and, if you, too, are victimized, or know someone who has been, the resources and advice provided in this book will prove invaluable.

---

Rodney D. Ryder book Introduction to Internet Law & Policy (A Course Book on Cyber Law, New Media Regulation & Policy, being Students Guide to Information Technology Act, 2000 E-Commerce, Data Protection & the Internet) the text is specially designed for courses in Internet or Cyber law, E-Commerce or Data Privacy Law. The book contains chapters on Evolution of Law in Cyberspace, A Perspective on Internet Related Legal Issues, Security Concerns, Trade Secrets and Privacy, Intellectual Property in Cyberspace, Digital Signature, Electronic Governance, Attribution, Acknowledgment and Dispatch of Electronic Records, Secure Electronic Records and Secure Digital Signatures, Regulation of Certifying Authorities, Digital Signature Certificates, Duties of Subscribers, Penalties and Adjudication, Data Protection, Tele-communication Regulations etc.

The text is specially designed for courses in Internet or Cyber law, E-Commerce or Data Privacy Law. The book contains chapters on Evolution of Law in Cyberspace, A Perspective on Internet Related Legal Issues, Security Concerns, Trade Secrets and Privacy, Intellectual Property in Cyberspace, Digital Signature, Electronic Governance, Attribution, Acknowledgment and Dispatch of Electronic Records, Secure Electronic Records and Secure Digital Signatures, Regulation of Certifying Authorities, Digital Signature Certificates, Duties of Subscribers, Penalties and Adjudication, Data Protection, Tele-communication Regulations etc., etc.

An accurate, analytic and informative text on an emerging legal topic. This book was created to offer a concise, current, and practical resource for understanding the legal environment of the Internet and electronic transactions. The author belongs to that select group of advocates who, as consultants to major national and international business concerns, have active experience of problems connected to the use of the internet as a critical tool of commerce and trade. The text is an authoritative survey of the existing and developing law relating to the internet, which is an indispensable tool, as well as, a vehicle for commerce, industry and trade today. In clearly and logically written chapters the author has covered a large number of inter-connected issues, including the creation of online agreements, legal risks involved in online businesses, data-protection and internet

banking, insurance, economics of the internet, cyber fraud, and defamation. The book includes analyses of relevant international and Indian cases. It has a detailed and extremely useful glossary.

*Karnika Seth book Cyber Laws in the Information Technology Age*¹ the prime objective of this book is to introduce its readers to the subject of cyber laws, elucidate key operative principles and to discuss the key developments in the field of cyber laws across many important jurisdictions-India, United States and European Nations. The book not only explains the fundamental concepts in cyberspace laws but also aims to present a fair overview of the evolution of cyber laws across many jurisdictions. The book discusses pertinent e-contracting and e-commerce issues, and describes popular e-payment systems and taxation regimes which are indispensable to e-commerce businesses. It elucidates the key principles for determining jurisdiction in cyber law disputes, significance of electronic signatures and admissibility of e-evidence, which are subject of interest to readers world over. This book also presents an insight into other interesting cyberspace issue such as online privacy, defamation, freedom of speech on internet, intellectual property piracy on internet, and cybercrime issues with case studies and landmark precedents from different parts of the world. It provides practical tips on safeguarding one's security and privacy in the online world and will enlighten readers on their legal rights and obligations in cyberspace and legal implications of their actions on the Internet. The book contains comparative assessment of cyber laws across different jurisdictions and critically comments on positive and negative traits of existing statutory framework, legal and policy framework and important judicial precedents in information technology law and regulation. Appendices of existing cyber laws, international conventions, treaties and guidelines framed by International Organizations pertaining to cyber law and intellectual property, important EU Directives and cyber legislations of India, US, UK and other foreign countries are also given for easy reference.

*Chris Reed book Internet Law Text and Materials*² this book explains the fundamental principles of law which apply to the Internet. It does this by (a) identifying the special legal problems which the Internet has created, (b)

¹ Ed. 2009, LexisNexis Butterworth's Wadhwa, Nagpur
examining the ways in which these are dealt with in different countries, and (c) identifying the common principles which are used globally to regulate use of the Internet.

Other books on Internet law explain the law of a particular country. This book is unique in that it examines the law globally. Its main importance is its fundamental analysis of legal problems and principles which are common to all countries.

From this analysis the reader will be able to understand the true nature of a particular legal problem, and thus be able to research and apply the appropriate national law rules to those problems.

*Cyber Crime — Issue threats and management is a masterwork by Atul Jain.*¹ His two volume work deals with a variety of subjects related to Cyber Crime. In volume 1, he speaks of subjects like nature, tactics, chronologies, consequences of cyber crime, global effort to combat cyber crime etc. This book offers a persuasive study of the damaging potential of cyber attacks on almost all aspects of human endeavor. It also describes the actions that need to be taken to control the threats from cyber attacks.

This book attempts to provide a greater understanding and awareness of the world of information insecurity and the impending natures of cyber-threats through the identification of the problem, potential solutions, and the development of an action plan. The book attempts to highlight the techniques that cyber-criminals are likely to use as their primary means of communication in the current state of the technology, such as untraceable emails, encryption, and digital compression.

This book is a useful and an interesting book to read for people who want to gather in-depth knowledge about cyber crime as it gives a good idea of what cybercrime is, how is cybercrime different from ordinary crimes, why is cybercrime difficult to tackle, what tactics do cyber offenders use, what are the consequences of cybercrime, what has been done by the world’s nations to tackle

cybercrime, what are the cyber crime laws around the world and throws light on several other relevant aspects.

Though, this book is interesting and is written in easy language, however, at some places, a reader who is a ‘complete’ layman in terms of computers and other related technology having no knowledge about the same may find this book complex because of the use of technical terms.

Prof. (Dr.) S.V. Joga Rao book Law of Cyber Crimes (Policy, Law & Practice along with the text of Global legislations focusing on Cyber Crimes, etc.)\(^1\) Takes within its fold, seventeen chapters and several appendices. The first chapter under the caption “Cyber Crimes: What do we know and What do we mean” deals with select cyber crimes, nature of criminal conduct that is involved and the extent of the impact a cyber crime creates. The second chapter focuses on different facets and divergent dimensions of Information Technology with a view to introduce its importance to the readers. Particularly, this chapter is meant for a non-technical person who desires to critically appreciate the niceties of IT’s importance. Third chapter addresses premises, issues and implications relating to technology and legal regulations. This chapter also takes within its fold select legal responses in cyber world. The fourth chapter in a detailed manner examines the inexplicable and inevitable interface between criminality and technology. The aim of this chapter is to clearly analyze in what way the forms of criminality in the context of technology have evolved over a period of time. Essentially, the prevalence, practice and terminological clarification pertaining to computer crimes and cyber crimes forms part of the core content of the fifth chapter.

Criminological insight with regard to cyber crimes is the essential focus in chapter six. Particularly, it explains the nature of multiple opportunities for cyber criminals and the factors hampering prosecution of cyber crimes and the challenges in controlling cyber crimes. This chapter analyses the need for a thorough and sustained criminological research from Indian perspective. The seventh chapter examines Typology of cyber crimes in a detailed manner. Valid issues pertaining to Criminalization in the context of cyber criminality have been addressed in the eighth chapter. In addition, pertinent principles of Criminal Law

have also been examined in a detailed manner. Chapter nine narratively explains different country legal responses focusing on the cyber crimes. Tenth chapter exclusively deals with a detailed analysis of Indian Legal response vis-à-vis cyber crimes. The eleventh chapter addresses the issues relating to criminal liability. Twelfth chapter examines the investigative aspects and procedures of cyber crimes. The thirteenth chapter deals with discovery, custody and presentment of cyber crimes related evidence.

The issues and implications regarding cyber crimes and Indian Criminal Justice Administration are covered in Chapter fourteen. An International initiative to combat cyber crimes is examined in the light of recent developments in Chapter fifteen. Chapter sixteen exclusively addresses the concerns and conflicts relating to Human Rights in cyber space. Finally, the seventeenth chapter critically outlays and analyses the way forward in the ambit of cyber crimes. The text of select global legislations focusing on cyber crimes have been covered in Appendices. This book is directed towards decision makers in both the private and public sector in hopes of the drafting and adopting of a comprehensive law of cyber space.

Stephen Dean book Sexual Predators: How to Recognize them on the Internet and on the Street - How to Keep Your Kids Away\(^1\) book is not a psychological or empirical evaluation of the techniques and methods used by online predators. It is not a report of a quantitative or qualitative study performed regarding child predators or victims of these adults. Rather, this book contains large portions of text that are actual accounts and conversations recorded by Dean, complimented by reported statistics of adolescent online use and characteristics of their predators. Dean’s purpose with this approach is to educate by real life experience and not through numbers and monotonous reports, as it can be assumed that he feels this would be the most effective way to reach his audience.

The first few chapters of the book provide examples of graphic conversations between persons posing as children and adults pursuing them for sexual encounters. Although readers may accuse the author of inserting these excerpts for pure shock value, the author’s intention is to demonstrate to adult online consumers the actual tactics being used on children in the privacy of their

\(^1\) Ed. 2007, Silver Lake Publishing, Los Angeles.
own home. For example, claims of shared interests or deceptions of age by the predators are often used as seduction tactics. The identification of the perpetrators in the text establishes that these predators can be well-respected members of the community, such as the orthodontist that was exposed in one of Dean’s investigations that tried to arrange a meeting for a sexual rendezvous with a 13 year-old girl. This further supports the notion that these prowlers are branching out beyond the stereotype.

The author spends an entire chapter discussing the concept of “grooming,” which is basically friendly flattery intended to win the trust of the child. This is often considered to be the first step toward sexual abuse of the victim. Dean provides not only different examples of grooming techniques, but also signs parents should be aware of that would show the grooming process. For instance, receipt of money or gifts in the mail from unknown sources are indications that improper communications with adults is occurring during computer time. Other indicators of improper chat room conversation are also listed, such as graphic sexual conversations or questions regarding a child and her respective parent’s daily schedule. Though many online consumers believe that these signs would be obvious to parent and child, there are many devious methods of developing a relationship with a trusting child that go unnoticed.

The book also reports on the various types of technology used by predators to gain access to children, some of which may not be expected by online consumers. Most users are familiar with chat rooms and instant messaging. Pedophiles tend to prey on adolescents in chat rooms by picking out screen names that would represent a young person. However, children often enter customized sexual chat rooms, such a homosexual or bondage room, basically under the premise of curiosity and adult prowlers quickly discover them. The sexual abuse that has resulted from these attacks has caused many chat room providers, such as MSNChat, to shut down or more stringently regulate its members and who is using its chat rooms. Instant messaging is a more private form of communication. Rather than using an arena where multiple persons are chatting on the same subject, instant messaging limits the viewing of a conversation only to its participants. Dean reported that over two-thirds of American teenagers use instant messaging,
many of which are contacted by unfamiliar persons in search of more than just a friendly chat.

Another technological device noted by Dean is the web cam. Although most people think that only they and the person they are chatting with can have access to their live images, anyone with a bit of hacking knowledge can gain entry into a personal computer and watch its users unnoticed. An example was given in the book of how an online predator watched a teenager girl’s daily activities, from dressing to doing homework, from the courtesy of her web cam perched on her computer. The girl never turned off the device, assuming only her friends could see her during chats, but this hacker proved her wrong.

An interesting point that Dean presents in his book is in regards to inadvertent corporate sponsorship of child sex chat rooms. Banner advertisements are purchased from Internet Service Providers (ISPs) and placed on the top or side of web pages. Since many corporations like to promote to younger generations (i.e. tennis shoes, soft drinks), a large portion of their advertisements are placed on chat rooms. The issue, however, is that they can appear alongside any chat room, despite the content or detail. The author gives the example of how a Brawny paper towel ad was placed in a Yahoo chat room named “Innocent Escapes,” which was actually a child sex room. Once the corporation discovered this mishap, it immediately pulled all the advertisements from the Yahoo system, but any reputation damage had potentially been done. The goal of this example is to dismiss any assumptions made by Internet users that the endorsements by popular and trusted brand names does not mean that the associated web site is appropriate. Although most people would not have imagined a simple grocery item such as paper towels would be associated with lewd sex acts, it can occur.

The final portion of the book is dedicated to explaining how the law responds to child sex crimes, as well how parents can take protective action in their own homes. Many police investigations are facilitated by parental awareness and evidence collected from home computers of emails, Instant messages and chat room transcripts. Dean is quite straightforward when he states that children operate under multiple screen names and identities to fool parents into seeing material that they know is inappropriate or prohibited. As a parent, Dean insists you have the right to infringe on your child’s computer privacy and should make
every effort possible to stay on top of their computer activity.

Although this book could be an informative tool for children, the text is geared toward the education of parents that may be naïve and unfamiliar with the newest technologies and the dangers that lurk online. Dean should be commended on his use of true life experience to demonstrate to his audience what disturbing events can truly happen once an online predator gains access to your home and your loved ones. It can be assumed that while these stories may have been implemented in the book as a shock technique, they also demonstrate reality better than hypothetical situations.

The reader will also find it valuable to take under advisory suggestions from Dean regarding his thoughts on penalizing a child that has participated in lewd conversations or devious behavior with an adult online. As most of us realize, children and adolescents can be rebellious creatures and completely forbidding them from computer use is only going to fuel their desire to do just that. Dean suggests keeping the computer in a common household room with a lot of traffic, constant monitoring of activity and restriction of certain areas on the Internet. Children should be educated on safe online use through actual experience with the Internet under adult guidance so that when they are left to their own devices, they will continue to be cautious.

There are also shortcomings to the book that could be improved. As stated before, a large portion of the book is composed of his experiences with online predator investigations in Houston, Texas. Based on his knowledge and experience, the author gives his own analysis of predator techniques and opinions of safety precautions for parents to heed. While this information is invaluable regarding what can be learned from these occurrences, there is rare scholarly support; empirical or otherwise. Occasionally dotted throughout the text will be a statement from a clinical psychologist or Internet resource group. However, there is a true deficiency in the fact that there is not a great deal of corroboration from other scholars in the field presented to demonstrate that Dean’s words have merit and are not just biased opinion.

Secondly, and although this lack may have been purposive by the author, suggested educational or therapeutic resources are absent from Dean’s book. It is apparent from the text that Dean has become quite an expert on online predators.
and there techniques. However, now that his book has educated his audience on different mannerisms and techniques of these predators, he makes no suggestion of what resources to seek if an adult online has violated someone in your home. For example, a chapter or section dedicated to listing information of counseling services for victims and the appropriate law enforcement agencies to notify are not noted in the book. The author is obviously extremely familiar with the topic and therefore should be familiar with outlets to manage the consequences of such a crime. This knowledge is just as valuable as the other information presented in the text.

Despite its limitations, this book would be an excellent read for a student of crime and/or information systems. The field of cyber crime is one that has yet to receive the attention and priority it deserves in academia and it is the responsibility of scholars to thoroughly understand this latest phenomenon in criminality. Advocates for the education of cyber crime are slowly influencing the incorporation of curriculum into degree programs. Dean’s repeated emphasis on the importance of this subject in the text, as well as examples of the result of inadequate education on predatory practices online, only provides further support that college graduates need to be equipped with this knowledge. Cyber criminality is becoming more and more a part of our daily lives, especially for those working in the fields of criminal justice and technology.

Overall, Dean’s book is a valuable contribution to the literature available to parents and all consumers on the dangers present on the Internet. Despite its similarity to other books published in the past, this book provides updated information, techniques and tactics that have just recently emerged into use by online predators. Legitimate computer programs and resources change on a daily basis, as well as the illegal aspects of technology that permit for the intrusion of privacy and safety; therefore, it is important for us as consumers to stay aware of the latest methods that are used. We cannot protect ourselves from entities we do not understand and Dean’s text helps to gear us in the right direction.

SIGNIFICANCE OF STUDY

This study is for the welfare of the society and government as it helps in the maintenance of law and order in the society as the study deals with the new crimes which are the result of new technology. Further, it also helps the business community by providing new technology in commerce. This will help the
government in collecting more taxes which are the result of adoption of new technology by the business community also this will provide transparency in the functioning of the government. If the suggestions mention in the study are adopted by the parliament this act will be a complete code.

OBJECTIVE OF THE STUDY
In the present study an attempt has been made to develop a 'cyber jurisprudence' having in view various cyber regulations made in India and other countries to check the cyber crime and the criminal. U.S.A, U.K., Malaysia, Singapore, Japan has been passed several new statutes to prevent cyber crime. While Indian Parliament have passed single Act, named Information Technology Act, for prevention of cyber crime. The object of study is to have a comprehensive analysis of cyber crimes, evaluate effectiveness of International as well as national control regime.

RESEARCH HYPOTHESIS
Information Technology Act, 2000 and Amendment Act, 2008 is not a complete code. There are many grey areas which require the attention of the legislature. Moreover, the amendments also left many lacunas in the Act. The lacunas in the Act, short coming in the investigation, new area of cyber crimes, new type of cyber crime and the new invention in the cyber technology made me to study the subject.

The logic of this hypothesis is the universal nature of the use, culture and system of internet or cyber space. Cyber crime is a 'boundary less' crime. Systems may be accessed in one country, the data manipulated in another country and the consequences felt in a third country. The result of this ability is that different sovereignties, jurisdictions, laws and rules will come into play. Therefore, the need for an analytical study of various legal control mechanisms and exploring the feasibility of a universal control mechanism, which is in conformity with the respective legal systems.

Certain topics arise in such a situation, which need to be dealt with :

- What is cyber crime and how can it be defined?
- To analyze the classification of cyber crime and the problem of conflicting laws on cyber crime and the jurisdictional limits imposed by International and national legal regimes.
• To study analytically, the cyber crime laws and to find out lacunaes.
• To evaluate world wide impact of cyber crime and Indian legal response.
• To analyze the process of investigation of cyber crime, Handling, labeling and compiling computer evidence and challenges in the investigation of cyber crimes.
• To analyze the international initiative for combating cyber crime.

RESEARCH METHODOLOGY

The research work is based on documentary and analytical methods. Data have been collected from secondary sources. Regarding the secondary sources information have been collected from books, judicial decisions, journals, articles, newspapers, magazines and Internet.

PLAN OF STUDY

The research has been presented systematically by dividing into seven chapters as under:-

Chapter-I gives the introduction of information technology, computer, Internet, Cyber space, Cyber Crime, definition of cyber crime, research hypothesis and object of study, research methodology.

Chapter-II contains History of Computer, Internet and Cyber crime. In 1960s, the United States Defence Department, Educational and Research Institutions started using internet facilities as their departmental network without any controlling measures. Founding fathers of Internet did not foresee cyber crimes and need of their prevention and control. Perhaps they thought that free use of cyber space would give scope for development. But the present socio-legal phenomenon is very different and complex and every moment cyber crimes are increasing.

Chapter-III contains classification of cyber crime. Classification of cyber crime is very complex task. Many writers on the subject have attempted many different typologies. Cyber crimes have been classified on the basis of the nature and purpose of the offence and have been broadly grouped into four categories. It may be affecting individual, economy, national security and contents based crimes. The list of cyber crimes is a newer-ending one; with each day never forms of criminal behaviour are being witnessed in the cyber world.
Chapter-IV deals with the reasons behind the increase in cyber crime, world wide impact of cyber crime. It explains the offences and penalties under Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008, admissibility of electronic evidence, Jurisdiction in cyber space.

Chapter -V contains Prevention and Investigation of Cyber Crime. The problems associated with cyber crimes are not limited to formulating substantive criminal laws. The unique characteristics of these types of crime make even the traditional procedural laws archaic. Also, these problems are not restricted to prosecution of cyber crimes alone but extend to many other fields of criminal investigation. The traditional rules of investigation and evidence collection are often useless in the investigation of cyber crimes. Coupled with this is the transnational nature of the crime. The criminal activity could be initiated in one country by accessing a system in another country and still, the result could be felt in many other countries. Also, the speed, absence of distance and borders, sophistication etc of the cyber space further complicates the investigation and prevention of cyber crimes.

Chapter-VI contains International Initiatives to Combat Cyber Crimes. Cyber crimes are not territorial crimes. Therefore, any isolated national efforts will not be successful in controlling cyber crimes. Thus, there is an urgent need to undertake steps towards increasing international coordination and cooperation in fighting cyber crimes.

Finally, based on the research, the conclusion has been drawn and few suggestions have been given for combating cyber crime in Chapter-VIII.