A. STATEMENT OF THE PROBLEM

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called ‘cyberspace’. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet.

The growing importance of Information Technology can be visualized from the fact that in India for the first time a Delhi based businessman has made a digital will of the secret information saved in his e-mail account. Digital will is a foreign concept which is gaining momentum in India also.\(^1\) Therefore, Internet has something to offer to everybody and in the process it only increases and never diminishes.

The ‘cyber manthan’ has bestowed many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few.\(^2\)

Despite such a great influence of computers and internet on day-to-day lives, the fact remains that only a fraction of people know what computer and internet is all about? There is a paucity of systematic study which elaborately discusses the basic concepts of cyber world like meaning, evolution, generations, types, characteristics and major components of computers; forms of networks, history of Internet in India, services and limitations of Internet etc.\(^3\) Most of the books and thesis directly deals with the concept of cyber crimes without thinking that to understand computer and internet crimes, one needs to understand first the computers and internet. This study is a sincere effort in this direction.

Well, the new medium which has suddenly confronted humanity does not distinguish between good and evil, between national and international, between just and unjust, but it only provides a platform for the activities which take place in human society. Law as the regulator of human behavior has made an entry into the cyberspace and is trying to cope with

\(^{1}\)“Ab E-mail Accounts Ki Bhi Hui Wasiyat”, Navbharat Times, April 5, 2010, p. 5

\(^{2}\)“Byte Replaces Bullets On Cyberspace”, Hindustan Times, September 18, 2006, p. 11

its manifold challenges. Though various countries have their domestic cyber laws, but the problem is that most of the books deal with cyber laws of individual nations. In this research work an attempt has been made to do a comparative study of the cyber laws of different countries.

A legal framework for the cyber world was conceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some of the provisions of our existing laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing cyber crimes, but the problem is that still this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology. Through this thesis the researcher has tried to interpret its technical provisions into simple language which can be understood even by laymen.

Since cyber crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace.

As a saying in criminology goes – “a crime will happen where and only when the opportunity avails itself.” Until recently, we were aware of only traditional types of crimes like murder, rape, theft, extortion, robbery, dacoity etc. But now with the development and advancement of science and technology there came into existence machines like computers and facilities like internet. The internet has opened up a whole new virtual heaven for the people both good and bad, clever and naive to enter and interact with lot of diverse cultures and sub-cultures, geography and demographics being no bar. The very same virtues of internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions, make it a virtual hell. Stories of copyright theft, hacking and cracking, virus attacks and plain hoaxes etc. have mounted up in the last few years. There is no single text available which provides a coherent and consistent exposition on the various categories of cyber crimes, their nature, scope, features and essential ingredients. It is fascinating to study cyber offences like cyber hacking, cyber fraud, cyber pornography, cyber terrorism,
cyber stalking, cyber ragging⁶ etc. and also the US, UK and Indian approaches towards these offences.

As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms. The law enforcement officials have been frustrated by the inability of the legislators to keep cyber crime legislation ahead of the fast moving technological curve. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world’s public and private networks. Moreover while investigating cyber crimes, the investigating agencies and law enforcement officials follow the same techniques for collecting, examining and evaluating the evidence as they do in cases of traditional crimes.⁷ Most of the books are silent on the issue of electronic evidence. In this study the researcher has critically analyzed the admissibility and evidentiary value of electronic evidence in addition to the methods of its procurement and examination.

Further complicating cyber crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major international organizations, like the OECD and the G-8, are seriously discussing cooperative schemes, but many countries do not share the urgency to combat cyber crimes for many reasons, including different values concerning piracy or espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another. Though the issue of jurisdiction in cyberspace cannot be settled spontaneously, but still a global effort in this direction is the need of hour.⁸ The present researcher has made an attempt to exhaustively analyze these jurisdictional riddles and has suggested the evolution of a uniform international law applicable to transnational cyber crimes.

Apart from tangible rights, some intangible rights called as ‘intellectual property rights’ such as trademarks, copyrights and patents etc. are also infringed in the cyberspace.

---


⁷ “Cyber Thieves are Caught, But Conviction is Wobbly”, Hindustan Times, August 9, 2006, p. 18

There is no dearth of specific books on IPRs, but books on IPRs vis-à-vis cyberspace are not much in number. This study has tried to undertake a collaborative approach on IPRs and cyber world.

The purpose of this study is to cover the complete scenario of internet crimes, their magnitude and nature, and make an insight into the people who are responsible for it. This research work will also take a comprehensive view of the governmental efforts being done in India and abroad to stop such crimes and will look closely on their success and failures.

An effort will also be made to vigorously analyze the various perspectives of IT Act, 2000; its ins and outs including its shortcomings and the possible means and ways to overcome them.

B. AIM, OBJECTIVES AND UTILITY

It is said that identifying a problem is what gives us power and energy to solve them as every problem has in it the seeds of its own solution. This statement signifies the need of defining the objective of research. The objectives of this research work are to touch all the important facets of the cyber crimes in a comprehensive way and to achieve new insights into it.

The main objectives of the present study are as under:
1. To understand the basic concepts of the cyber world.
2. To trace the origin and development of the cyber crimes.
3. To examine critically the position of intellectual property rights in cyber space.
4. To analyze the principles of jurisdiction in cyber offences.
5. To discuss comprehensively the concept of electronic evidence.
6. To decipher as to how the issue of cyber crimes has been dealt with in the Indian scenario.
7. To find out the international initiatives to curb cyber menace.
8. To point out the possible defects and loopholes in the existing laws relating to cyber crimes.
9. To suggest the reforms and remedial measures for the prevention and control of cyber crimes.

The main aim is to study the judicial interpretation of the prevalent cyber laws at the global level. The endeavour is to determine all the important facets of cyber crimes in various countries of the world including UK, USA and India. The study also attempts to find possible
implications of the recently evolved cyber crimes. The significance of the study is to decipher the cyber law as developed in India as well as to do critical comparative analysis of the cyber laws as developed in other countries.

The study is important both from the theoretical and practical point of view. On a theoretical level, it reveals the judicial appreciation of all the important facets regarding cyber crimes. On the practical level, it clearly shows the extent to which judicial approach meets the requirements of the day by protecting the people against various cyber offences. The result of the study would provide hitherto unknown criteria to evaluate the legislative and judicial philosophy in the research area.

The practical utility of the work lies in the fact that policy making institutions may remove ambiguities surrounding the cyber laws. They may also enact specific cyber legislations pertaining to cyber crimes.

C. OVERVIEW OF THE EXISTING LITERATURE

They say books are the most quietest and most constant of friends, they are the most accessible and wisest of counselors, and the most patient of teachers. No thesis can be written without consulting good books and articles. One of the steps for starting the work on the problem is to review the existing literature on the subject. After identifying a problem, it is imperative to consult literature on the subject as the answers you get from literature depends on the questions you pose. The review of the existing literature not only provides clarity of concept and understanding of different aspects of the subject but also helps avoid repetition. It helps in identifying problem zones. It also helps in formulating research methodology. A number of books, monographs, reports, research papers and articles deal with the subject of prevention and control of cyber crimes.

1. India

i. Books

a. Justice Yatindra Singh in his book “Cyber Laws” has elaborately discussed the meaning and importance of intellectual property rights like trademarks, copyrights, patents etc. vis-à-vis cyber space. According to him, these rights refer to the property

---

that is a creation of the mind i.e. inventions, literary and artistic works, symbols, names, images, and designs used in commerce.\(^\text{10}\) As far as the infringement of IPRs in cyberspace is concerned he has critically analyzed the judgments of *Napster Case*,\(^\text{11}\) *Sony Play Station Case*\(^\text{12}\) and *Grokster Case*.\(^\text{13}\)

b. Vivek Sood in his book “*Cyber Crimes, Electronic Evidence and Investigation: Legal Issues*”\(^\text{14}\) has suggested various strategies to curb cyber crimes. He says that since cyber crimes are technology based, so the best answer to these crimes is security technology.\(^\text{15}\) Fire-walls, anti-virus software and anti-intrusion systems are some of the effectively used security technologies. He concluded that “protect yourself” is the best *mantra* against cyber crimes.\(^\text{16}\) According to him, effective cooperation between the law enforcement agencies within the country and between nations is also necessary to challenge cyber criminals and bring them before the law. Further he calls for strengthening of extradition treaties and their implementation as a must in this digital age.

c. Dr. Vishwanath Paranjape in his book “*Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India*”\(^\text{17}\) has pointed out that with the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue.\(^\text{18}\) He has suggested the need for international cooperation to combat cyber crimes and in this regard he has comprehensively discussed various national and international conventions, conferences, summits etc. relating to cyber crimes along with the municipal cyber legislations of different countries like UK, USA, India, Canada, China, Japan, Germany, Australia, and France etc.

\(^{10}\) *Id.* at p. 45


\(^{12}\) Kabushiki Kaisha Sony Computer Entertaining v. Stevens, 2002 FCA 906

\(^{13}\) MGM Studios Inc. v. Grokster Ltd., 545 US 193


\(^{15}\) *Id.* at p. 172

\(^{16}\) *Id.* at p. 173

\(^{17}\) Dr. Vishwanath Paranjape, *Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India*, Central Law Agency Publication, 2010

\(^{18}\) *Id.* at p. 166
d. **Nandan Kamath** in his book “Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000” has commented on the emerging field of ‘electronic evidence’ in the cases of cyber crimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and of certain other concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rule etc.

e. **Dr. M. Dasgupta** in his book “Cyber Crime in India: A Comparative Study” has succinctly defined the meaning, nature, scope, characteristics and elements of cyber crimes. Commenting on the scope of cyber crimes he has stated that “it is very essential to emphasize that the world is not run by weapons anymore, or energy, or money. It is run by ones and zeros….little bits of data ….it is all electrons. There’s a war out here, a world war. It is not about who has the most bullets. It is about who controls the information – what we see and hear, how we work, what we think etc. it’s all about information.” Further, he has critically analyzed the modus operandi of some important cyber crimes like cyber hacking, cyber terrorism, cyber pornography, cyber fraud etc. and also stated the national and international initiatives to prevent and control such cyber crimes.

f. **S.K. Verma and Raman Mittal** in their book “Legal Dimensions of Cyber Space” have explained the basic concepts of cyber world like meaning, types, features and major components of computers; history and development of internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. Emphasizing on the importance of computers and internet in day-to-day chores they have opined that “today it touches and influences almost every aspect of our lives. We are in the information age and computers are the driving force. We hardly do any activity that is not in some way dependent on computers.” They further suggest that not only do we need to be computer-literate, but we also need to

---

20 *Id.* at p. 52  
22 *Id.* at p. 8  
23 S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute Publication, 2004  
24 *Id.* at p. 1
understand the myriad issues that surround our extensive and necessary dependence on computers. Commenting on the interlink of human-conflicts-law, they states that where humans are, crime and conflict of interests cannot be far behind, further, where crime and conflict of interests are, law must necessarily march in order to take control and regulate. Thus, they have made a detailed study on the indispensable role of computer and internet, and the resultant cyber crimes.

g. Vakul Sharma in his book “Information Technology; Law and Practice” has evaluated the issue of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made references to various principles like territorial principle, nationality principle, protective principle, passive personality principle, effects principle and universality principle. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length.

h. Rodney D. Ryder in his book “Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet) has exhaustively dealt with the provisions of the Information Technology Act, 2000 as amended in the year 2008. He has pointed out some grey areas of the Act and has also suggested the remedial reforms in order to provide more teeth and nail to the Act.

i. R.K. Chaubey in his book “An Introduction to Cyber Crime and Cyber Law” has emphasized on the significance of ‘right to privacy’ in digital age, stating that the new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of eavesdroppers. Thus, individual privacy is at greater stake than ever before. Computers and the internet can be used to amass huge amount of data regarding people, profile it in various ways, modify it and

25 Id. at p. 2
26 Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., 2010
27 Id. at p. 251-53
28 Id. at p. 257
29 Id. at p. 260
deal with it in a manner which could violate individual’s privacy.\textsuperscript{32} He has examined the concept of privacy in the light of various national and international laws. He also discusses how the practices commonly used on the internet like cookies, web bugs, spamming could lead to the violation of privacy. Also, he has highlighted the importance of adopting privacy policy by websites.

\textbf{j. V.D. Dudeja} in his book \textit{“Cyber Crime and the Law”}\textsuperscript{33} has highlighted the interplay of freedom of expression and the internet. Enumerating the reasonable restrictions on the freedom of expression he has concluded that in the interests of privacy and security some restrictions can also be put on the use of computers and internet because law has been able to recognize computer as a ‘weapon of offence’ as well as a ‘victim of crime’ leading to the emergence of cyber jurisprudence.\textsuperscript{34}

\textbf{ii. Articles}

\textbf{a. Agarwal, S.C.,} in his article \textit{“Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements”},\textsuperscript{35} has stated that the law enforcement officials throughout the world are severely handicapped in tackling the new wave of cyber crimes. He has gone to the extent of saying that you “either have to take a cop and make him a computer expert or take a computer specialist and make him a cop”.\textsuperscript{36} He has suggested that we have to set up a Cyber Crime Investigation and Training Cell in all the States for imparting training to the police personnel, public prosecutors and judicial officers.\textsuperscript{37}

\textbf{b. Ahmad, Farooq} in his article \textit{“Interplay of Internet Domain Names and Trademark Law”},\textsuperscript{38} has observed that internet domain names have spawned unprecedented legal issues which do not have express solution. Though the courts have accorded equal protection to trademarks and domain names, but still domain names are at stake due to highly technical nature of computers and internet. He has given a detailed account of

\begin{itemize}
  \item \textsuperscript{32} \textit{Id.} at p. 108
  \item \textsuperscript{33} V.D. Dudeja, \textit{Cyber Crime and the Law}, Commonwealth Publication, 2002
  \item \textsuperscript{34} \textit{Id.} at p. 168
  \item \textsuperscript{35} Agarwal, S.C., \textquote{“Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements”}, \textit{CBI Bulletin}, 2001 Feb.; p. 4-11.
  \item \textsuperscript{36} \textit{Id.} at p. 8
  \item \textsuperscript{37} \textit{Id.} at p. 11
  \item \textsuperscript{38} Ahmad, Farooq, \textquote{“Interplay of Internet Domain Names and Trademark Law”}, \textit{Indian Bar Review}, 2001 Apr.-Sep.; p. 233-92.
\end{itemize}
the role of Uniform Domain Name Dispute Resolution Policy (UDRP) in protecting
domain names. 39

c. **Behra, Abhimanyu** in his article “Cyber Crime and Law in India”, 40 has discussed
various types of cyber crimes and also suggested strategies to curb them.
d. **Dalal, A.S.** “Jurisdiction in Cyberspace”, 41 has elaborately examined the
jurisdictional issue in trans-border cyber crimes and calls for an effective international
regime to tackle the recently evolved cyber menace.

e. **Fatima, Talat** in her article “Liability of Online Intermediaries: Emerging
Trends”, 42 has opined that though the intermediaries are unconscious actors in the
internet transaction and they have no pre-existing legal relationship with other actors,
still they are duty-bound to take precautionary measures for preventing cyber
crimes. 43 She has made an exhaustive study on the civil, criminal and tortuous
liability of the intermediaries. 44

f. Muddaraju, N. and Ramesh in their article “Cyber Crimes: Need an Effective
Law”, 45 has emphasized on the need for specific cyber legislations to effectively deal
with cyber crimes.
g. **Nagpal, Rohas** in his article “Offences and Penalties under the Information
Technology Act, 2000”, 46 has made a critical study of various cyber crimes and
Corresponding penalties provided under the IT Act. He has also pointed out some
loopholes in the Act and suggested measures to make it more effective.

---

39 Id. at p. 274
Apr.-Jun.; pp. 155-78.
43 Id. at p. 155
44 Id. at p. 158
227-31.
46 Nagpal, Rohas, “Offences and penalties under the Information Technology Act, 2000”, *Information
h. Paranjape, Vishwanath in his article “Cyber Crime: A Global Concern”,\(^{47}\) has focused on the global nature of cyber crimes and also presses the need for global measures to curb them.

i. Ramesh in his article “Pornography and Obscenity on the Web: Need a Strict Law”,\(^{48}\) has raised the issue of relevance of morality in cyber space by stating that obscene and pornographic materials online has the tendency to deprave innocent young minds.\(^{49}\)

ej. Sharma, Anupam in his article “Globalization and its Impact on Cyber Crime: Case Study of Indian Police Administration”,\(^{50}\) has examined the impact of globalization, liberalization and privatization on the cyber crimes and concluded that more advancement in technology leads to highly technical nature of the crimes.

iii. Miscellaneous

a. Law Commission Report

The Law Commission of India in its 188\(^{th}\) report on “Proposals for Constitution of Hi-Tech Fast-Track Commercial Divisions in High Courts” have recommended the creation of “Commercial Division” in each of our High Courts so that they may handle commercial cases of high threshold value of say Rs. 1 crore and above, or such higher limit as may be fixed by the High Court on a fast-track basis. It has further recommended that a maximum period of 2 years is perfectly justified and is comparable to the period of pendency in most countries abroad and in particular United Kingdom and United States of America. It adopted the definition of “Commercial Cause” as stated in Rule 1 of Part D of Chapter III (Part V) of the Delhi High Court Rules, with slight modifications and stated that “Commercial Causes” includes amongst other causes the commercial disputes arising out of software, hardware, networks, internet, websites and intellectual property such as trademark, trademark.


\(^{49}\) Id. at p. 23

copyright, patent, design, domain names and brands. A list of few other reports consulted for the present study is mentioned in the reports section of the bibliography.

b. **Websites**

A number of standard websites such as those of Internet Corporation for Assigned Names and Numbers, Indian Ministry of Information Technology, World Intellectual Property Organization etc. were visited and consulted for information on various issues. A detailed list of the websites is given in the internet reference section of the bibliography.

c. **Newspapers**

Some national dailies like The Hindu, The Times of India, The Indian Express, The Tribune, The Hindustan Times etc. were also read for latest news regarding cyber crimes. A list of these dailies is given in the newspaper section of the bibliography.

d. **Magazines**

The legal magazines like Lawyer’s Update, Practical Lawyer, and Lawyer’s Collective etc. were consulted for updated information on cyber scenario. A list of such magazines is provided in the magazine section of the bibliography.

2. **United Kingdom**

i. **Books**

a. **Albert, J. Marcellai and Roberts S. Greenfield** in their book *Cyber Forensics- A Field Manual for Collecting, Examining and Processing Evidence of Computer Crimes*, have made a coherent and comprehensive study on various aspects of the electronic evidence including its collection, examination and evidentiary value. They have carved out an altogether new discipline of cyber forensics while focusing on cyber crimes and cyber law.

b. **Brian, Loader and Douglas, Thomas**, in their book *Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age*, has emphasized

---

52 www.icann.org
53 www.mit.gov.in
54 www.wipo.net
on the enforcement of cyber crime legislations by stating that “proper enforcement of law in its letter and spirit is more important than its enactment.”\textsuperscript{57} Further, they have focused on the enhanced role of law enforcement agencies in investigating cyber crimes.

c. Chissick, Michael and Kelman, Alistair in their book “Electronic Commerce- Law and Practice”,\textsuperscript{58} have stated that e-commerce is a new way of conducting, managing and executing business transactions using modern information technology. They have efficiently explained the meaning of new business nomenclature like “Business-to-Business’ (B2B), ‘Business-to-Consumer’ (B2C), ‘Consumer-to-Business’ (C2B), and ‘Consumer-to-Consumer’ (C2C) etc. which has come into existence in the recently emerged e-environment.

ii. Articles

a. Bigos, Oren in his article “Jurisdiction over Cross-Border Wrongs on the Internet”,\textsuperscript{59} has stated that internet knows no boundaries. He has critically analyzed the issue of jurisdiction in cyber offences and advocated that an international law universally applicable to all the countries of the world is the need of hour to nip the evil of cyber crimes in the bud itself.\textsuperscript{60}

b. Finkel, E.D., in his article “Cyberspace under Siege”,\textsuperscript{61} has addressed the issue of cyber security in the context of e-environment. He has opined that “cyber security is a team sport that we all need to play effectively”. Emphasizing on the balance between indispensable roles of information technology and the need for cyber security, he has borrowed creepy cockroach metaphor to bring the point home by stating that “the philosophical approach that you have to take is not how to stamp out all the cockroaches, but how do you live the rest of your life in a room full of cockroaches?”

3. United States of America

i. Books

\textsuperscript{57} Id. at p. 198
\textsuperscript{58} Chissick, Michael and Kelman, Alistair, Electronic Commerce- Law and Practice, Sweet & Maxwell, London, 2000
\textsuperscript{60} Id. at p. 616
has succinctly examines the concept, history, evolution and modes of cyber terrorism. While equating cyber terrorism as a crime against humanity he has critically analyzed the global initiatives taken to prevent and control cyber terrorism.

has discussed the cross-border nature of cyber crimes. He has stated that the cyber criminals treats the entire world as one home and carry on their nefarious activities which have transnational ramifications.

c. **Stephenson, Peter** in his book *“Investigating Computer-related Crime”*,
observed that traditional methods of investigating traditional crimes are of not much use in the investigation of hi-tech crimes committed on e-way. Thus, he has enumerated various modes, methods and techniques to investigate the crimes committed via computers and internet.

ii. **Articles**

a. **Christopher, R. Perry** in his article *“Trademarks as Commodities: The Famous Road Block to Applying Trademark Dilution Law in Cyberspace”*,
has emphasized on the importance of domain names in cyber space and also discussed the role of Uniform Domain Name Dispute Resolution Policy in the cases of infringement of domain names.

b. **Decker, Charlotte** in his article *“Cyber Crime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime”*,
has called for updating the US Criminal Code to meet the recently evolved and challenging branch of cyber crimes stating that existing laws are outdated as far as computer crimes are concerned.

**D. RESEARCH METHODOLOGY**

---

The methodology of research differs according to the subject. This study is doctrinal in nature. An attempt has been made to make a comparative analysis of cyber laws of various countries. This monograph is an attempt in the direction of getting a world view of cyber crimes by studying an approach to it at the international level. The material from decided cases of courts of United Kingdom, United States of America and India has been used. The basic data has been drawn from the decided cases from the High Court and House of Lords in United Kingdom, United States District Courts, United States Court of Appeal, U.S. Supreme Court, and the High Courts and Supreme Court of India. The cases have been drawn from AC, AIR, All ER, Ch. D, CTMR, FSR, PTC, RPC, SCC, USPQ, WLR etc. As the scope of the subject is vast and ever expanding with regular output of decisional material from the courts, a representative selection of cases from United Kingdom, United States of America and India has been made to cover all the important aspects of the chosen problem. A list of cases has been given for ease of reference to the reader.

E. CHAPTER SCHEME
The present research work has been divided into nine chapters.

1. **Chapter I – ‘Introductory’** articulates the problem for study in the area of cyber crimes. It describes the methodology employed and gives an overview of literature.

2. **Chapter II – ‘Basic Concepts of the Cyber World: An Overview’** gives an account of some general aspects of the cyber world such as meaning and salient features of cyberspace, cyber criminal and cyber law; meaning, evolution, generations, types, characteristics and major components of computers; types of networks, evolution of Internet, history of Internet in India, services and limitations of Internet; malicious computer codes like virus, Trojans, worms etc.

3. **Chapter III – ‘Cyber Crimes: Meaning, Definition, Nature, Scope, Elements, Characteristics and Classification’** analyses the definition of cyber crimes as given by renowned authors and jurists. The present researcher has examined the nature, scope, characteristics, essential elements, and classification of cyber crimes on various bases and also the factors responsible for cyber crimes. It also incorporates an analytical and evaluative study of some important cyber crimes like cyber hacking, cyber fraud, cyber pornography, cyber stalking, cyber defamation, cyber terrorism etc. and also the international, UK’s, USA’s and Indian initiatives to prevent and control
these cyber crimes. A general overview of the approach of judiciary of UK, USA and India towards these cyber crimes have also been highlighted in this chapter with the help of case laws.

4. **Chapter IV – ‘Intellectual Property Rights in the Cyber Space’** examines various intellectual property rights in cyber space like trademarks (domain names), patents and copyrights and also the criterion and procedure for their registration. It also enumerates the modes of infringement of these intellectual property rights and the remedies available to their owners.

5. **Chapter V – ‘Jurisdiction and the Internet: A Global Medium in a Territorial World’** throws light on the issue of municipal law vis-à-vis international law and jurisdiction in cyber space. It also covers the concepts of prescriptive, enforcement, territorial and extra-territorial jurisdiction in the cases of cyber crimes. Further, a deep insight has been made into the question whether cyber crimes are extraditable offences? It states the US, European and Indian approaches towards the personal jurisdiction in cyber offences. Moreover, the applicability of the Brussels Regulation and Rome Convention in the online environment with regard to jurisdictional aspect has been discussed at length.

6. **Chapter VI – ‘Electronic Evidence: Tracking Digital Footprints’** intends to evaluate the evidentiary regime vis-à-vis Internet. The concepts like video-conferencing, admissibility of electronic records, burden of proof, rule against hearsay, best evidence rule, primary versus secondary evidence, public versus private documents etc. have been dealt with extensively in the context of electronic evidence.

7. **Chapter VII – ‘Statutory Provisions regarding Cyber Crimes in India: The Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008’** makes an exhaustive study about the provisions of the Information Technology Act, 2000 as amended in the year 2008 which is the statutory law on the subject of information technology, of which cyber crimes is an offshoot.

8. **Chapter VIII – ‘Global Perspective of Cyber Crimes and the related Laws’** discusses the need for international cooperation to combat cyber crimes. It takes into
account various Conferences, Conventions, Summits, and Treaties on the subject of cyber crimes and cyber laws, with special emphasis on the Twenty-second G-7 Summit on Cyber Crime (1996), Paris Cyber Crime Conference (2001), European Convention on Cyber Crime (2001), International Conference on Cyber Crime (2007), Conference on Cyber Security and Protective Strategies (2009), International Conference on Digital Forensics and Cyber Crime (2009), Fifth Annual Conference on Cyber Crime (2010), and Fourth International Conference on Cyber Law etc. It briefly discusses the cyber laws of various countries like US, UK, Canada, Australia, Germany, Turkey, Japan, France, Spain, Russia, China, Sri Lanka, Bangladesh, Pakistan etc. It also focuses on the international agencies like World Trade Organization (WTO), World Intellectual Property Organization (WIPO), and Internet Cooperation for Assigned Names and Numbers (ICANN).

9. **Chapter IX – ‘Conclusions and Suggestions’** addresses the conclusions and suggestions arrived at as a result of the discussions in the previous chapters. An attempt has been made to point out the shortcomings and lacunae in the cyber laws and to suggest remedial measures to ensure effective prevention and control of the cyber crimes. The seeking is the goal and research is the answer. It is believed that the thesis may throw light on the subject of cyber crimes in a holistic way. It is earnestly hoped that the conclusions drawn and the suggestions presented on the basis of critical study in this discourse will be a real contribution to the field. It is said that the best way to become acquainted with a subject is to write a book on it. The present research work is only an attempt to understand the cyber crimes by making a comprehensive analysis of the cyber crimes and relevant cyber laws of various countries with main focus on Indian scenario.