A. INTRODUCTION

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. 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.

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 its manifold challenges. 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.

Moreover 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. 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.

B. OBJECTIVES OF THE STUDY

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.

C. RESEARCH METHODOLOGY

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 to make a comprehensive study on the prevention and control of cyber crimes.

D. SCHEME OF CHAPTERS

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’**

dresses 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. Based on the study following suggestions are recommended:

1. Net Security be tightened up
2. Use of Encryption Technology
3. Intrusion Management
4. False E-mail identity registration be treated as an offence
5. Self-regulation by Computer and Net Users
6. Liberalization of Law relating to Search and Seizure
7. Use of Voice-recognizer, Filter Software and Caller ID for Protection against Unauthorized Access

8. Development of Cyber Forensics and Biometric Techniques


10. Need for a Universal Legal Regulatory Mechanism


12. Need for Universalization of Cyber Law

13. Interpol and Emergency Response Computer Security Team

14. Combating the Menace of Cyber Terrorism

15. Special Cyber Crime Investigation Cell for Hi-Tech Crimes

16. E-Judiciary and Video-Conferencing for Speedy Justice

17. Need for Cyber Crime Reporter or Cyber Law Journal

18. The Information Technology (Amendment) Act, 2008 – A Step in the right direction

19. Digital Time Stamping System (DTS)

20. Extradition Treaty: Need of the Hour

21. Establishment of Special Cyber Courts to try Cyber Crimes

22. Diffusion of Internet Technology in India

23. Technical Means for Blocking of Errant Websites

24. Planting of Baits in Cyberspace for Worms and Viruses

25. Regulation of Social Networking Sites

26. Decentralization of the National Informatics Centre
27. Appointments under the IT Act, 2000: Fair, Transparent and Speedy
28. Need for Increased Awareness among Victims of Cyber Crimes
29. Need for Imparting Training to Officials to Investigate Cyber Crimes
30. Need for connecting Cyber Cafes with Police Control Rooms
31. Periodical reviewing of licenses of Internet Service Providers (ISPs)
32. Need for Development of Anti-hijacking Software
33. Encouragement of Cyber Crime Victims to Lodge Complaints
34. Need for Modernization of Existing Laws and Enactment of New Laws
35. Implementation of the Recommendations of Malimath Committee on Reforms in the Criminal Justice System
36. Computer and Cyber crime: Education and Awareness