CHAPTER-1

INTRODUCTION

“If I had an hour to save the world I would spend 59 minutes defining the problem and one minute finding solutions”.

Albert Einstein

1.1 Statement of the Problem

The digital technology gives a space to everyone. This space is known as cyberspace, which provides a separate space for their activities. Internet is being used about in all activities of daily life including communication, commerce, advertising, banking, education, research and entertainment. There is hardly any activity that not touched by the internet. In few words, it can be said that the Internet has entered into the blood of the human beings. It has been found that many of the young got addicted to remain online all-time.

Internet has blessed the human species with many gifts associated with the pitfalls. As this space has no boundary and gives a super secure space for all kinds of unlawful activities. The traditional terrorism gets new wings of internet. Now it is very easy to perform the very sophisticated attacks without visiting that targeted place. Now, in this cyber world, it is very difficult to trace the actual culprit. It provides a space for the human activities but without thinking the just and unjust.

The internet age gives a new world to the new types of weapons and target as well to the terrorists. It also gave a new shape to the ways that terrorist group’s structure and operates their organizations\(^1\). Zanini and Edwards, had found, the most infamous terrorist organizations on the path of information technologies, and also

using hi-tech machines to organize and coordinate activities. Internet, wireless communications, and other computer networks pose various new challenges for law enforcement agencies throughout the world.

The computerization of all sectors invites the vulnerability. As the saying is clear in criminology, - “a crime will happen where and only when the opportunity avails itself.” And at the same time, ‘once you connected, you are vulnerable’ is very much true. So in the same way use of internet provides more chances to the cyberterrorists to accomplish their bad ends.

It cannot be denied that internet technology has given a new speed to the development. At the same time law enforcement agencies started their task but failed and frustrated because of the peculiarity or the nature of the cyber terrorism. They found themselves unable to adhere with the fast growing technology. On the other hand, 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.

Most of the works on cyber law are silent on the issue of cyber terrorism. In this study the researcher has analyzed the instances and critical infrastructures vulnerable to attack, laws and policies of different countries on cyber terrorism.

Since cyber terrorism is not a matter of concern of India only. The countries also have framed their rule and statues. Various countries have their domestic cyber laws, but the problem is that most of the books deal with cyber laws of individual

---

2 Ibid.
4 “Cyber Thieves are Caught, But Conviction is Wobbly”, Hindustan Times, August 9, 2006, p. 18.
nations. In this research work an attempt has been made to do a comparative study of the cyber laws and policies of different countries.

The purpose of this study is to cover the complete scenario of cyber terrorism, 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 made 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.

1.2 Objectives of the Study

The research/study seeks to achieve the following objectives:

1. To understand the basic concepts of the cyber world.
2. To trace the origin and development of the Cyber crimes.
3. To trace the origin and development of the cyber terrorism.
4. To understand the critical infrastructure, vulnerable to cyber attack.
5. To analyze the law and policies of India to curb cyber terrorism in the Indian scenario.
6. To find out the international initiatives to curb cyber menace.
7. To investigate the possible defects and loopholes in the existing laws and policies relating to cyber terrorism.
8. To suggest the reforms and remedial measures for the prevention and control of cyber terrorism.

The basic motto of the study is to analyze the cyber laws at the global level. It is an endeavour to determine all the important facets of cyber terrorism in various countries of the world including UK, USA, Japan and India, etc. The study also is an attempt to find possible implications of the recently cyber attacks.
1.3 Rationale of the Study

The significance of the study is to decipher the most critical infrastructure which affects the pulse of any country. And further an analysis of cyber law as developed in India as well as to do critical comparative analysis of the cyber laws as developed in other countries relating to the cyber terrorism.

The study is important both from the theoretical and practical point of view. On a theoretical level, it reveals the legal and policy appreciation of all the important facets regarding cyber terrorism. On the practical level, it clearly shows the extent to which legal and policy 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 terrorism.

1.4 Limitation of the Study

Seeking to achieve the above stated objectives the study however as any other study is subject to following limitations

1. The greatest limitation of this study has been lack of higher order knowledge of computer and internet required for deeper understanding of technicalities of cyber space. However researcher has undertaken the endeavour to accumulate working knowledge of computer and internet.

2. The study has to be confined primarily to cyber terrorism. However, it will be incomplete without the discussion of the other crimes in cyber space.

3. There is no consensus on the definition of cyber terrorism, so it is tried to collect the possible approaches relating to cyber terrorism.
4. The nature of the topic is every vast so the study laws and policies of all countries is not possible. So the research is based only on the selected countries’ laws and policies.

5. The cyber attacks in the cyberspace are not easy to trace and criminals may be out of reach of law and administration. So, there are less number of cases of cyberattack without any arrest or prosecution.

1.5 Hypothesis

The present legal and policy framework for addressing or curbing the cyber menace of cyber terrorism is not robust to achieve the avowed objectives of:

i. Protecting the critical infrastructure.
ii. Effective response to the cyber terrorism.
iii. Build confidence in cyberspace.

1.6 Research Methodology

This present work is doctrinal work hence major study has been in library. The data and information has been collected from both primary and secondary sources.

Constitution, Acts, treaties, subordinate legislation, orders of tribunals and courts, Reports of various committees has been looked into as primary sources. The cases decided by various judicial and quasi-judicial forums have been also analyzed for internal and external consistencies. Internal consistencies here means consistencies vis-a-vis that particular issue amongst various case situations, external consistencies means consistency vis-a-vis statutes, guidelines, rules etc. Proceedings of conferences, both National and International on issues pertaining to response to the cyber terrorism have been relied upon as secondary sources. Also books, articles, journals, reports and monographs discussing the issue has been looked into as secondary sources. E-resources have been extensively referred to. Help has been taken from law firms and institutions also. Moreover the opinions, observations,
perceptions and philosophies of the eminent authors, lawyers and jurists in the area have been looked into.

The tool of doctrinal research which has been applied is descriptive and qualitative ones. Descriptive studies have been undertaken to ascertain anecdotal events, working of institutions and behavioural patterns of groups. It has been employed to understand research problem. The purpose of this study was to enhance predictability under certain circumstances. Qualitative research has been employed to analyze cases, makes a comparative study of the various systems.

The materials collected from primary and secondary sources have been presented in descriptive manner and wherever required critical inputs have been provided.

Although work is strictly a doctrinal one, Empirical data from both primary and secondary sources have been used in the study. However, neither a field study nor data collection through questionnaires of formal interview was undertaken. Even though there were many informal meetings with many experts in the field, they have not been cited in the work because all arguments are based on published materials. For the purpose of interpretation of legislations secondary sources were relied upon.

Further, foreign legislations have also been made basis of the present study. Comparative study of laws of the U.K., the U.S.A., Japan, and Australia were also done to get a better perception and understanding of various provisions of Indian legislations.

1.7 Review of the Literature

They say books are the 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 and of cyber terrorism.

The review of existing literature on the topic has its limitations, so the available and approachable number of books, monographs, reports, research papers and articles has reviewed for the better understanding of concept.

a. Books

i. Justice Yatindra Singh in his book “Cyber Laws”\(^5\) provides a comprehensive guide to the various legal issues which have arisen as a result of the unprecedented growth of the internet. It covers both academic and practical information regarding technology related issues and the underlying legal principles which have been applied in these areas. The book provides an overview of the cyber law scenario in India. In the book many aspects have been discussed very nicely.

The book covers all the important changes introduced by the IT (Amendment Act) of 2008. The book also incorporates several important provisions of the Communication Convergence Bill of 2001. As far as the infringement of IPRs in cyberspace is concerned he has critically analyzed the judgments of Napster Case,\(^6\) Sony Play Station Case\(^7\) and Grokster Case\(^8\). The cyber terrorism has been discussed but in brief, even though the book is a nice work on the issues of cyber space and intellectual property rights.

ii. Vivek Sood in his book “Cyber Crimes, Electronic Evidence and Investigation: Legal Issues”\(^9\) has suggested various strategies to curb cyber

\(^7\) *Kabushiki Kaisha Sony Computer Entertaining v. Stevens*, 2002 FCA 906
\(^8\) *MGM Studios Inc. v. Grokster Ltd.*, 545 US 193
crimes. He says that since cyber crimes are technology based, so the best answer to these crimes is security technology. 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. The book inter-alia deals with various strategies to effectively counter these new-age crimes, explains the stepwise process of leading electronic evidence in the Court, analyses the various provisions of the I.T. Act, 2000 & IT Amendment Act, 2008 & other related statutes, takes a firm view on challenging legal issues on the subject and also answers the question whether India should sign the Convention on Cyber crime.

iii. Dr. Vishwanath Paranjape in his book “Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India” 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. The book suggested the need for international cooperation to combat cyber crimes and cyber terrorism. The book also comprehensively discuss 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.

iv. 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

---

10 Ibid p. 172.
11 Ibid p. 173.
13 Ibid. p. 166.
of certain other concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rules, etc. The book also discusses the latest trends and crimes in the cyber space.

v. 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.

vi. 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 understand the myriad issues

---

15 Ibid. p. 52.
17 Ibid. p. 8
19 Ibid. p. 1.
that surround our extensive and necessary dependence on computers. Commenting on the interlink of human-conflicts-law, they state 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\textsuperscript{20}. Thus, they have made a detailed study on the indispensable role of computer and internet, and the resultant cyber crimes.

vii. Vakul Sharma in his book “Information Technology; Law and Practice”\textsuperscript{21} 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\textsuperscript{22}. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals\textsuperscript{23}. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length.\textsuperscript{24}

viii. Rodney D. Ryder in his book “Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet)”\textsuperscript{25} 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.

ix. R.K. Chaubey in his book “An Introduction to Cyber Crime and Cyber Law”\textsuperscript{26} 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

\textsuperscript{20} Ibid. p. 2.
\textsuperscript{22} Ibid. pp. 251-53.
\textsuperscript{23} Ibid. p. 257.
\textsuperscript{24} Ibid. p. 260.
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 data in various ways, modify it and deal with it in a manner which could violate individual’s privacy. 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.

V. D. Dudeja in his book “Cyber Crime and the Law”\(^{28}\) 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.\(^{29}\)

Albert, J. Marcellai and Roberts S. Greenfield in their book “Cyber Forensics- A Field Manual for Collecting, Examining and Processing Evidence of Computer Crimes”,\(^{30}\) 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. According to the book, Cyber Forensics includes details and tips on taking control of a suspect computer or PDA and its “operating” environment, mitigating potential exposures and risks to chain of custody, and establishing and following a flowchart for the seizure of electronic evidence. An extensive

\(^{27}\) Ibid. p. 108.


\(^{29}\) Ibid. p. 168.

list of appendices also provides, which include websites, organizations, pertinent legislation, further readings, best practice recommendations, more information on hardware and software, and a recap of the federal rules of civil procedure.

xii. Loader Brian and Thomas Douglas, in their book “Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age”,\(^{31}\) have emphasized 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.”\(^{32}\) Further, they have focused on the enhanced role of law enforcement agencies in investigating cyber crimes.

xiii. Michael Chissick and Alistair Kelman in their book “Electronic Commerce-Law and Practice”\(^{33}\) 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.

xiv. Bary C. Collin, in his book “The Future of Cyber Terrorism”,\(^{34}\) 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.

xv. James R. Richards in his book “Transnational Criminal Organizations, Cyber Crime and Money Laundering”,\(^{35}\) has discussed the cross-border nature of cyber crimes. He has stated that the cyber criminals take the entire world as


\(^{32}\) Ibid. p. 198.


one home and carry on their nefarious activities which have transnational ramifications.

xvi. Peter Stephenson in his book “Investigating Computer-related Crime”, has 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.

b. Articles

i. S.C. Agarwal in his article “Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements”, 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.” 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.

ii. Abhimanyu Behra in his article “Cyber Crime and Law in India”, has discussed various types of cyber crimes and also suggested strategies to curb them.

iii. A.S. Dalal “Jurisdiction in Cyberspace”, 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.

---

38 Ibid p. 8.
39 Ibid. p. 11.
iv. Talat Fatima in her article “Liability of Online Intermediaries: Emerging Trends”,\textsuperscript{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\textsuperscript{43}. She has made an exhaustive study on the civil, criminal and tortuous liability of the intermediaries\textsuperscript{44}.

v. N. Muddaraju and Ramesh in their article “Cyber Crimes: Need an Effective Law”,\textsuperscript{45} has emphasized on the need for specific cyber legislations to effectively deal with cyber crimes.

vi. Vishwanath Paranjape in his article “Cyber Crime: A Global Concern”,\textsuperscript{46} has focused on the global nature of cyber crimes and also presses the need for global measures to curb them.

vii. Anupam Sharma in his article “Globalization and its Impact on Cyber Crime: Case Study of Indian Police Administration”,\textsuperscript{47} 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.

viii. E.D. Finkel in his article “Cyberspace under Siege”,\textsuperscript{48} 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

\textsuperscript{43} Ibid. p. 155.
\textsuperscript{44} Ibid. p. 158.
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?”

ix. Charlotte Decker 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.

c. Miscellaneous

i. 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.

ii. 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. Some other dailies of United States, UK and other countries, available online, also read for the latest updates on the research topic. A list of these dailies is given in the newspaper section of the bibliography.

50 www.icann.org.
51 www.mit.gov.in.
52 www.wipo.net.
iii. 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.

1.8 Operationalization of Terms/Expressions

There are certain terms which have been used throughout the study. These terms have also been defined and explained in greater detail at the appropriate places. Unless specified otherwise, for the purposes of studies the terms described refers to the following.

1.8.1 Cyber Space

The term ‘cyber space’ was first used by William Gibson in his science fiction ‘Neuromancer’ in 1982, which he later described as “an evocative and essentially meaningless buzzword that could serve as a cipher for all of his cybernetic musings. Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. Thus, ‘cyberspace’ is the electronic medium of computer networks, in which online communication takes place and where individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussions etc.

1.8.2 Netizen

Persons in cyberspace are called netizens i.e. anyone who is associated with computers, information technology and the Internet. Thus, a netizen is a person who becomes part of and participates in the larger internet society, which recognizes few boundaries save language. The term ‘netizen’ comes from the combination of two
words ‘Internet’ and ‘citizen’. The number of netizens had jumped to 700 million in 2001 from a mere 143 million in 1998 and according to a UN report, world will have 2.7 billion netizens by the end of 2013 which is about 39 per cent of the global population were connected to internet and this number is increasing at a very fast speed every year. The report said that in the developing world, 31 per cent of the population are online, compared to 77 per cent in the developed world. Sub-Saharan Africa, where less than 20 per cent of the population is using the internet, remains the region with the lowest penetration rate. Further there are over one billion websites online.

1.8.3 Computer

The term ‘computer’ is derived from the word ‘compute’ which means to calculate. A computer is an electronic machine devised for performing calculations and controlling operations that can be expressed either in logical or numerical terms. It performs various operations with the help of instructions to process the information in order to achieve desired results. Further endless complex calculations can be done in mere fraction of time. Huge data can be stored without any space problem. Communication has become cheaper, faster and easier. Similarly difficult decisions can be made with unerring accuracy at comparatively little cost.

Today computers are widely seen as instruments for future progress and as a tool to achieve sustainability by way of improved access to information by means of

---


video-conferencing and e-mail. Indeed, computers have left such an impression on modern civilization that we call this era as the ‘information age’\textsuperscript{56}.

1.8.4 Networks

The value of a computer increases when it is connected to other computers. It is just like a telephone. If A has telephone then he can use his phone to call any of his friends provided all his friends have telephone. Hence, where his friends are not having telephone then it is useless for A to have telephone. Similarly, where A has computer it will be more useful for him in case it is connected to other computers. This connection among the computers constitute network. Therefore, a network is a collection of computers that are connected through a communication channel i.e., cables, fiber optics, etc. to share data, hardware and software\textsuperscript{57}.

1.8.5 Internet

The term ‘Internet’ is derived from two words ‘interconnection’ and ‘networks’. Internet is a worldwide system of computer networks i.e., network of networks which allows the user to share information on those linked computers. It consists of thousands of separately administered networks of various sizes and types. Each of these networks comprises number of computers. LANs are connected by using public switched network to create a WAN and when number of WANs and other interconnected networks such as intranet and extranet are connected, it results in Internet. All computers connected to the Internet communicate to each other only by using a common set of rules which are known as protocol. For this communication, each computer should have its own address which is called as IP address\textsuperscript{58}.

1.8.6 The World Wide Web

The World Wide Web (abbreviated as WWW or W3, commonly known as the web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks. The web was developed between March 1989 and December 1990\(^{59}\).

1.8.7 E-mail

It is the oldest application of the internet comprising exchange of digital information between two internet users. It is an asynchronous one-to-one communication. It is the most useful part of the internet and perhaps its greater boon. Letters across the seas taking days or weeks pass on to the other end of the world like a flurry though it is not always true and often a technical lacuna may delay it. The e-mail first was initially exchanged on the ARPANET to the FTP but it is now carried by Simple Mail Transfer Protocol (SMTP). In the beginning, it was “instant messaging “which required both the sender’s and receiver’s PC to be “on “position but now “store and forward” is more acceptable.

1.8.8 Critical Infrastructure

Critical Infrastructure (CI) is defined as an asset, system or part thereof located in a nation which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in that nation as a result of the failure to maintain those functions\(^{60}\).

---


1.8.9 Cyber Crime

The new millennium brings new crimes. Cyber crime can be regarded as “computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks”. Cyber crime is a crime which committed by the criminals in a cyber environment using Internet, computer networks, and wireless communication systems as a tool or target. In other words, cyber crime involves crime committed through use of the computer. Department of Justice (DoJ) (1989) as defined cyber crime as “any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution”.

1.8.10 Terrorism

“An act of terrorism, means any activity that (A) involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; and (B) appears to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by assassination or kidnapping.”

1.8.11 Cyber Terrorism

Cyber terrorism is the use of electronic networks, and computer technology, as a weapon. Attacks through the Internet need to have a terrorist component in order to be labeled “cyber terrorism.” For the historical purpose, the word “cyber terrorism” was born in the late 1980s when Collin, a senior research fellow at the

---

Institute for Security and Intelligence (ISI) in California,\textsuperscript{64} coined this hot techno-
phrase by combining two linguistic elements: cyberspace and terrorism.

The United Nations (UN) Counter-Terrorism Implementation Task Force 
(CTITF), although not explicitly using the term cyber terrorism, recognizes that one 
of the ways a terrorist organization may use the Internet is the “use of the Internet to 
perform terrorist attacks by remotely altering information on computer systems or 
disrupting the flow of data between computer systems.”\textsuperscript{65}

The concept of ‘pure’ cyber terrorism is related to those terrorist activities that 
are carried out entirely (or primarily) - in the virtual world. The Internet provides 
many different ways of anonymously meeting with ‘like minded’ individuals in a 
(comparatively) safe way. Furthermore, a successful cyber terrorism event could 
require no more prerequisite than knowledge-something that is essentially free to the 
owner once acquired, and an asset that can be used over and over again.

\section*{1.9 Scheme of Chapterisation}

The thesis on “Cyber Terrorism: Law and Policy” consists of following 
chapters:

\begin{enumerate}
\item Chapter 1

\textbf{Introduction} – The first chapter introduces the topic, research issues and 
explains the parameters of the research work and the underlying approach in 
identifying the issues. It describes the methodology employed and gives an overview 
of literature. It dwells upon the development of cyber crime and cyber terrorism, 
elaborates the focus of the study followed by the method adopted for research into the 
issue chosen.

\textsuperscript{64} B. Collin, “The Future of Cyberterrorism”, Proceedings of 11\textsuperscript{th} Annual International Symposium on 
Criminal Justice Issues: The University of Illinois at Chicago, 1996.

\textsuperscript{65} U.N. Counter-Terrorism Implementation Task Force, Report of the Working Group on “Countering the 
Use of the Internet for Terrorist Purposes”, 8 (February 2009), Available on 
ii. Chapter 2

**Evolution and Classification Cyber Crimes and Cyber Terrorism** - Second chapter gives an account of general aspects of the cyber world such as meaning and salient features of cyberspace, characteristics of Cyber crimes, cyber criminal and cyber attack; causes of cyber crimes; classifications of cyber crimes; malicious computer codes like virus, Trojans, worms etc. A brief discussion on cyber terrorism also has given.

iii. Chapter 3

**Bulging Dimensions of Cyber Terrorism** - Chapter three dedicated to the concept of Cyber Terrorism to understand it in a holistic way. It analyzes the concept of terrorism, cyber terrorism and its evolution, definition, characteristics, elements, terms related to the cyber terrorism, modes of cyber terrorism, and incidents of the cyber terrorism and new perspectives of the cyber terrorism. In this chapter the cause of attractiveness and current state of attack is also discussed.

iv. Chapter 4

**Critical Infrastructure** – Chapter four of the research focuses on the critical infrastructure in India or of any country, which attracts the cyberterrorists. It deals with the kinds of critical infrastructure, characteristics of it, and the possible threats to the critical infrastructures. It also analyzes the actors threatening and also the measurements have taken by the stakeholders worldwide.

v. Chapter 5

**International Legal Response to Cyber Terrorism** – Chapter five deals with the legal response to cyber terrorism. The main focus of this chapter is on the conventions and conferences on cyber terrorism and their response and conclusions
on the study. Statutory provisions of various countries, including Canada, Japan, UK, USA, Spain, Pakistan and India, etc. has given.

vi. Chapter 6

Policy Response to Cyber Terrorism – This exclusive chapter discusses the policy of various countries to curb the menace of cyber terrorism. The issue of non-consensus on cyber terrorism also gets it due place in this chapter. The current status of the policy on cyber terrorism also has been discussed. In the light of the limitation of the study only selected countries policy has discussed in this chapter, including USA, United Kingdom, Japan, and India.

vii. Chapter 7

Conclusion 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 and cyber terrorism. The seeking is the goal and research is the answer.

It is believed that the study may throw light on the subject of cyber terrorism 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 terrorism by making a comprehensive analysis of the cyber crimes, cyber terrorism and relevant cyber laws and policies of various countries with main focus on Indian scenario.