CHAPTER I
INTRODUCTION
CHAPTER I

INTRODUCTION

1.0 General Introduction

When Blaise Pascal built the first non-electronic computer in 1642, little did he know that centuries later the descendants of this innovation would change the way we live and would rewrite law lexicons. These electronic behemoths became a substitute for human brains. In 1969, the birth of the internet multiplied the power of this wonder machine and the world was never like before. New crimes appeared and old crimes disappeared, and what counts as a crime will vary across the societies. The creation of new crimes may be most evident in times of rapid social, political, economic, technological and cultural change, as unseen forms of human activity and interaction has become possible, bringing with them challenges and threats to order and well being.

The rapid development of internet stands as an example of such change, just ten years ago it was in its infancy, yet it is now a fact of life for billions of people around the globe. It has brought in its wake significant changes in the ways we work, trade, study, learn, play, consume, communicate and interact. At the same time, a whole host of crime problems has emerged in tandem with life online. Politicians, police, businesspeople and citizens now have a new vocabulary with which to identify such dangers, hacking, spoofing, phishing,
viruses, Trojans, malware, piracy, downloading, spyware, chat room grooming, and so on.

The internet has opened up a world of opportunities in e-commerce and information sharing, on the flip side the internet has its own threats and abuses which are perpetrated by a new breed of criminals known as cyber criminals. Just as you know that our world is unsafe and criminals lurk in dark alleys, in the cyber space too criminals lurk and the danger is all the more high with new and novel methods employed by cyber criminals.

With the internet being touted as no one being in-charge and one can do whatever one wants, cyber criminals started having a field day with a range of crimes like cyber terrorism, cyber stalking, cyber warfare, invading your privacy, cyber pornography or obscenity etc.

The world is indeed, undergoing a new information revolution today. It not only touches every aspect of life but also makes the way extensively to perform the industrial and economic function of the society. New communication system and digital technology have made dramatic changes in the way we live. A revolution has been occurred due to technological progress. Almost everybody is making substantial use of computers and the internet are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier. They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life.
Computers and the Internet continue to pervade human life in everything from automobiles to kitchen appliances. With the invention of computers, its increasing use and human dependency over Internet, while we have gained manifolds in terms of efficiency and management, it has also brought to the front many negative effects and disadvantages. Individuals or groups can now use Cyberspace to threaten International governments, or terrorize the citizens of a country. The crime of "cracking" can escalate into terrorism when an individual "cracks" into a government or military-maintained website. Cyber-terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage for an act of revenge.

1.1 Computer crime or an e-crime

The computer crime or an e-crime can be simply defined as a crime where a computer is the target of a crime or it is the means adopted to commit a crime. While some of the crimes may be new, the others are simply different ways to commit conventional crimes such as frauds, theft, blackmailing, forgery, and embezzlement using the online medium often involving the use of internet. What accelerate the growth of such crimes are typical characteristics of cyber space inter alia anonymity, speed, access, dependency, borderless space and lack of awareness of laws.

The information technology is a double edged sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions, as the case may be, of the person
dealing with and using the technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, etc can bring only destructive results. These methods, however, may also be used for checking the authenticity, safety and security of one’s technological device, which has been primarily relied upon and trusted for providing the security to a particular organisation. For instance, the creator of the “Sassier worm” has been hired as a “security software programmer” by a German firm, so that he can make firewalls, which will stop suspected files from entering computer systems. This exercise of hiring those persons who are responsible for causing havoc and nuisance is the recognition of the growing and inevitable need of “self protection”, which is recognised in all the countries of the world. In fact, a society without protection in the form of “self help” cannot be visualised in the present electronic era. The content providers, all over the world, have favoured proposed legislations in their respective countries, which allow them to disable copyright infringers’ computers. In some countries the software developers have vehemently supported the legislations which allows them to remotely disable the computer violating the terms and conditions of the license allowing the use of the software. This position has, however, given birth to a debate about the desirability, propriety and the legality of a law providing for a disabling effect to these “malware”. The problem is further made complicate due to absence of a uniform law solving the “jurisdictional problem”. The Internet recognises no boundaries; hence the attacker or offender may belong to any part of the world, where the law of the offended country may not be
Introduction

effective. This has strengthened the need for a "techno-legal" solution rather than a pure legal recourse, which is not effective in the electronic era.¹

Almost everybody is making substantial use of computer. The giant companies, now small companies/firms also are investing millions of rupees in sophisticated information system. Railway, Banks, Judiciary etc. are the institutions which are computerised and there are many departments/institutions/ministries which are trying to achieve the goal of "fully computerised". In fact we are living in the "Information age" through automation and development in the field of communication.²

On one hand, the information store in electronic form has many advantages like storing, retrieving, communicating but on the other hand it has opened the door to anti social and criminal behaviour in the way that would never have previously been possible. Computer systems often some new and highly sophisticated opportunities for law breaking, and they create the potential to commit the traditional types of cases in non-conventional ways. The rapid transactional expansion of large scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity of misuse to the criminals. For this, the security of computer based information system requires serious consideration especially in the light of reports of various cyber crime i.e. cyber

¹ http://www.cuisine-research.org/articles/1873/6 (visited on April 24, 2008).
terrorism, information of theft, data accessing, hacking etc. There is a need for
the law enforcement officials to know the various aspects of computer related
crimes- whether they are computer targeted crimes or computer assisted crime
or crimes in which computer is incidental to the crime. Investigation of these
crimes requires high technical skill. Conducting effective searches and seizures
and converting computer files into evidence are challenging task for the law
enforcement officials^{3}.

Success in any field of human activity leads to crime that needs
mechanisms to control it. Legal provisions should provide assurance to users,
empowerment to law enforcement agencies and deterrence to criminals. The
law is as stringent as its enforcement. Crime is no longer limited to space, time
or a group of people. Cyber space creates moral, civil and criminal wrongs. It
has now given a new way to express criminal tendencies. Back in 1990, less
than 100,000 people were able to log on to the Internet worldwide. Now around
500 million people are hooked up to surf the net around the globe.

Until recently, many information technology (IT) professionals lacked
awareness of and interest in the cyber crime phenomenon. In many cases, law
enforcement officers have lacked the tools needed to tackle the problem; old
laws didn’t quite fit the crimes being committed, new laws hadn’t quite caught
up to the reality of what was happening, and there were few court precedents to
look for guidance. Furthermore, debates over privacy issues hampered the

^{3} Ibid.
ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy or at the least, distrust between the two most important players in any effective fight against cyber crime, law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users.

The high rate of incidence and frequency with which the cyber crimes occur have made the makers all over the world to sit up and take notice. Cyber savvy nations concerned about their netizens online safety have come with a slew of legislations to bring the perpetrator to book. However, this is only a beginning, since the cyber laws in most countries are in a nascent stage and are still in the process of evolution. This means that it would take a while before they are made fool proof and adequate in containing cyber criminals.

1.2 Statement of the Problem

The real issue is how to prevent cyber crime. For this there is a need to raise the possibility of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenges in cyber crime cases include getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries. The police have to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is
based on the evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals, but from our ignorance and what is needed is the will to fight it. The law is stricter now on producing evidence. Specially where electronic documents are concerned.

Under Indian Law, cyber crime has to be a voluntary and wilful act or omission that adversely affects a person or property. The Information Technology Act 2000 provides the backbone for e-commerce and India’s approach has been to look at e-governance and e-commerce primarily from the proportional aspects. Looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age, there is a need to take into consideration the security aspects. In the present global situation where cyber control mechanisms are important, we need to push cyber laws. Cyber crimes are a new class of crimes to India due to rapidly expanding extensive use of internet. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Many police stations in various parts of India have computers, which are connected to their respective head quarters. Cyber police stations are functioning in major cities all over the country. The pace of the investigations can become faster, judicial sensitivity, and knowledge need to improve. Focus is needed to sensitize our investigators and judges to the importance of the system.
1.3 Objective of the study

The objectives of the present study are as follows:-

i) The main object is to specify the e-danger. The legal world familiar with theft and murder but now it is smuggling to macro terrorism from selling secrets to subverting systems from hijacking to hackling. The face of time has undergone a big change, its definition has changed its modus operandi has changed and the perpetrators are no longer Lombroso’s bearded and hard looking criminal but a white collar criminal a fiddler or by an egomaniac.

ii) The object of this research is to highlight the formidable problems face by the legal world, which have raised their heads due to information explosions. If cyber space is left ungoverned, it will lead to disastrous end where cyber space shall turn into veritable Siberia where greed, gambling, pornography and sex will reign supreme. The object is therefore to circumscribe within the limits of research work problem like jurisdiction question, overlapping of laws, multiplicity of laws, transnational nature of cyber crimes and various problems relating to investigation and lack of visual evidence.

iii) Emphasis has been made to educate the investigating officers, prosecutors and judges about the need for amending the existing provisions of penal law to ensure efficiency in prosecution and trials.
iv) Measures adopted by various countries including the U.S. the home land of the internet other western countries having a high standard of connectivity and convergence are more vulnerable to cyber crime, thus they have a good number of cyber acts. India too passed IT Act 2000 and other relevant Acts. The object is to analyse various legislations in this area and to explore the possibilities of a stricter legal framework.

In view of the above descriptive realities there is a need for having a serious study of the whole scenario to identify the main issues and find out solutions of the problems. There are various laws in Indian scenario keeping in mind the position of cyber crime in India. We can be benefited by looking at American and European experiences that have been battling for the right position till date.

1.4 Hypothesis

The research carried on the following hypothesis;

There is no comprehensive legislation in our country which deals with cyber crimes. Cyber crime has entered into popular demonology and today no one can claim to remain in affected by it as individuals, business organizations, governments & states all are in the net.

The judicial system in our country is not conducive to affective enforcement of any law as a result the laws have failed to achieve their objectives. Our legislature is yet to respond to seriousness related to cyber crimes.
Computer and Information technology revolution has brought in unprecedented advantages to the society. The exponential growth of internet has change live of the people. There is no sphere of human endeavour, which remains untouched by the information technology while the technology is ushering in all round economic progress, bestowing great benefits to the humanity. The criminal activities are not lagging behind, suddenly a set of new criminal activities called cyber crimes has become a new challenge to the society. No longer the nation states can sit and watch this phenomenon. In some aspects computer crime is much more dangerous than traditional crime. It is easy to commit and difficult to prevent.

i) It is hypothesized that the law has prohibited the phenomenon of cyber crimes but the operation of law has no preview over the cyber criminals.

ii) Cyber crime is a socio legal problem and various difficulties arise in investigation and legal framework. So there is a need of a sufficient legislation to prevent this social evil.

iii) How the internet has become a dangerous area for children and finally strategies, nations are adopting in combating this crime.

iv) That despite of adequate safeguards and number of legislations the problem of cyber crime continues unabated because of the poor machinery in our country and the major problem of jurisdiction.
v) The problem is multi-fold and it covers the crime related to economy as well as other crimes such as pornography which has its basis, certain moral standards and uses parameters like indecency and obscenity.

1.5 Research Methodology

Law is a normative science that is, a science which lays down norms and standards for human behaviour in a specified situation or situation enforceable through the sanction of the state. What distinguishes law from other social science is its normative character. This fact along with the fact that stability and certainty of law are desirable goals and social values to be pursued, make doctrinal research to be of primary concern to a legal researcher. Doctrinal research, of course, involves analysis of case law, arranging, ordering and systematizing legal propositions, and study of legal institutions, but it does more it creates law and its major tool (but not only tool) to do so is through legal reasoning or rational deduction.4

The present study is based on the doctrinal method of research. The researcher has drawn help from various books, Articles, newspapers, gazettes, report of commissions and committees and judicial decisions.

1.6 Literature Review

The literature available on the subject reveals that there are a number research studies being conducted on the cyber crime and its impact on the

---

Introduction

society. Most of the studies have tried to find out the menace of cyber crime and its possible control through the available legislation. The studies tried to find out that, how the cyber crime are committed and what are the distinctive modes of controlling them in the interest of the society. Another important observation is that an overwhelming number of studies have adopted the method of content analysis.

R. K. Chaubey (2009)\(^5\) Cyber crime is the latest type of crime which affects many people. It refers to criminal activity taking place in computer networks, knowingly or intentionally, access without permission, alters, damage, deletes and destroys the database available on the computer or network. It also includes the access without permission to the database or programme of a computer or network in order to devise or execute any unlawful scheme or wrongfully control or obtain money, property or data. It poses the biggest challenge for police, prosecutors and legislators.

Justice Yatindra Singh (2012)\(^6\) The proper analysis of Cyber Laws, the author lucidly explains the science behind the technology in order to sort out the legal issues. The internet has introduced another technology known as webcasting or internet broadcasting which involves streaming of audio/video on internet called internet radio. These are retransmission of over the air broadcasts through internet. The internet has brought forward a new class of persons, known as intermediaries, who provide physical facilities to transmit or

---


route the information, also known as Internet Service Providers. The study is an asset to companies dealing in computer software or providing software solutions, web page providers, Internet service providers, Banks, Insurance companies and other bodies providing online services, government departments implementing information technology, police officials dealing with investigation of cyber-crimes, teachers, students, lawyers and judges.

**Vakul Sharma (2004)**: The study comprise of numerous illustrations, concept notes and examples make the subject interesting and comprehensible. It attempts to interpret the true legislative intent behind the Act by referring to and applying the Supreme Court judgments for better assimilation and understanding of its various provisions relating to cyber crime.

The author has tried to assimilate the thoughts of Judges, Lawyers, Civil Servants, Police Officers, Technocrats and Students whom he met during his public lectures, discussions, workshops, seminar across the length and breadth of the country over the past many years.

The critical appraisal of powers and functions of the Cyber Regulatory Appellate Tribunal, Controller of Certifying Authorities, Adjudicating Officers and Police Officers under the Information Technology Act has been attempted.

**Chris Reed (2000)**: Other available materials on Internet Law explain the law of a particular country. This work 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 the analysis of the book *supra* the researcher have been 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 that problem.

**Nandan Kamath (2008):** The Internet has emerged as a medium with immense potential, posing many new and interesting challenges. There have been many attempts to regulate and control this medium, especially through the laws and regulations. This exciting publication explores the various aspects of cyber law and cyber regulations, taking the reader through a multitude of legal and policy issues that the Information Age poses. Topics covered in this book range from evidentiary aspects and digital signatures to intellectual property concerns such as copyright liability and rights in domain names; from cyber crime and cyber porn to the regulation of free speech on the Net and the right to privacy. A new chapter on Cases on Computers, Internet, e-mail etc. have been added. Employing a comparative law approach, this book, in its fourth edition, not only takes into consideration the changes brought about by the Information Technology Act of 2000, but also contains the latest developments alongwith a comprehensive guide to this legislation. Being wide-ranging as well as in-depth in its coverage of Indian Cyber law, this publication is a must-read for judges, lawyers, Policy makers, researchers, investigators and students as it is for

---

anyone who would like to keep abreast of new developments in the legal system, concerning Information Technology.

Pavan Duggal (2013)\textsuperscript{10} The emerging developments in cyber law along with the dark side of Internet and the world wide web and its consequent legal consequences have made the thing interesting in understanding the cyber crime and its control mechanism. Cyberlaw is a phenomenon has evolved in our own lifetimes. In the last decade and a half, huge developments have taken place which impacts every user of a computer, computer resource and communication device. Cyberlaw is one of the latest and most complex disciplines of legal jurisprudence.

1.7 Presentation of the Study

The present study is comprises of seven chapters including introduction, conclusion and suggestions.

\textit{Chapter First} related with Introduction refer the problem of cyber crime and cyber terrorism in India. It contain the review of literatures that provide a bird's eye view of the research conducted in the field of cyber crime and cyber terrorism. It also explain the statement of the problem, hypothesis formulated for the purpose as well the objectives of the study and methodology adopted to conduct the research work. \textit{Chapter Second} deals with conceptual analysis of cyber crime. In this chapter history and evolution of cyber crime has been

discussed in detail. Categories of sub crime and their sub categories also explained with the help of case laws.

*Chapter Third* is divided into two parts. First part deals with the defamation in which the position of various countries has been taken and the punishment as prescribed by different legislation of that particular country. The second part of this chapter is related to hacking. In this part various types of hacker has been discussed and the punishment prescribed by the law is also taken for the study. *Chapter Fourth* is devoted with the study of obscenity and pornography. In this chapter the researcher has attempted to discuss about the obscenity, pornography and its impact on children and adolescents. This chapter also highlights the porn business and the income there from in various countries.

*Chapter Fifth* discusses cyber crime against government. In this chapter terrorism through the internet and the reasons why the terrorist choose this medium to terrorize the government in particular and peoples in general has been discussed. The protection mechanism is also suggested in this chapter, either through technological or by legislation medium. *Chapter Sixth* is devoted for legal and technological measures that has been suggested to combat the cyber crime and cyber terrorism. In this chapter various issues of internet, like the impact of market value, consumer trust, potential economic impact etc. has been taken into consideration. Through the analysis of these, the measures have been suggested for protection and improvement.
Chapter Seventh caption Conclusion & Suggestions Where in the researcher made a modest but sincere efforts to conclude the study of the cyber crime and cyber terrorism in India and also made some humble suggestions to control the menace of cyber crime and cyber terrorism through various ways and means.