Chapter 1

INTRODUCTION
Chapter 1

INTRODUCTION

1.1 Introduction

The present age is the age of automation where man is shifting his maximum burden on machines for getting work done. The Computer Technology helps the human civilization to such a great extend that life without computers seem to be impossible! The Railway reservations, Space organizations, Examination result cards, Traffic signals, Telephonic communications, Banking transactions, all are now carried out with the help of computer machines and every data and information has acquired electronic shape and capable to move through the optic fibers. Today, voice files, song files, photographs, currencies, news items, clips, bio-data's, letters, so on and so forth are capable of being transferred, distributed, circulated and stored in electronic form.

The way cyberspace is being experienced by people in the very disparate contexts of their everyday lives is matter of growing concern. It is mediated by the technologies of the digital age and encompasses a wide range of issues including the production and consumption of digital content, the means of control over unwanted intrusions to individual’s privacy, and emerging means of basis of transaction influencing to real world too. Globally and locally today’s information societies are underpinned by digital technologies. These technologies enable applications that may be empowering for some people, allowing them to develop new ways of seeing the world around them. Ubiquitous networks are at the heart of the digital age. They are becoming familiar to people in all parts of the world, albeit, unevenly so. Thus present generation is greatly depends upon the computer technology for the easy mechanism and effective operations.

However, the facilities of computer technology have not dawn into reality without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime'. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misleading with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds. Today computers have come a long way, with
neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications.¹

Therefore, it is necessary to examine the deadliest form of criminality of the present millennium, conceptually termed as 'Cyber crime'.

1.2 Initial remarks: Crime and Law as a social phenomenon

At the very outset of this research writing, it must be made clear that the present study has been focused to study from Indian point of view upon the -

i. Legal control of Cyber crime - as well as

ii. The problems that are emerging with ever-growing use of Cyber Technology, and -


It is, therefore, essential that the scope and area of the subject must be outlined at initial stage. As conventionally understood, both crime and law is a social phenomenon having inter-correlated dependency. The rate of crime commissions (or omissions as well!) is largely determined by the efficiency of controlling and regulating legal machineries.

Thus speaking in statistical sense, crime rate is inversely proportional to the efficiency of regulatory legal mechanism. To check crime rate, legal machinery can be focused upon. Evidently, both law and crime is productivity of social process. In short, to carry out the research writing on the subject entitled, 'Legal control of Cyber crime in India: Problems and Prospects', restricted legal approach may not lead to comprehensive study. As both crime and law have several dimensions apart from social one.

1.3 Evaluating Crime - Socio-Political-Economical

1.3.1 Crime as an evil factor of society

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritable by the question, *Why there is too much ado about crime?*

No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behaviour! However, it should bear in mind that the social concern for high crime rate is not because of it's nature, but due to potential disturbance it causes to the society.

Crime is a prime social concern and the seriousness of the social effect of crime hardly needs to be described. The general public is, by definition, always been the victim of crime. The general public suffers losses from crime either directly (in the treason or theft and destruction of public property), or indirectly (in the form of the expense of maintaining the police and the courts and in the form of uneasiness or even terror because of the prevalence of crime). In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

Therefore there is sentiment of hate for crime, which reflects into the form of prescription of punishment by political authority of given society. The crime is considered as evil for the society. The statistics reflects the growing incidences of crime in India, though there is stiff downfall under the crime rate under Indian Penal Code, 1860 (due to the increase number of special legislation). The graph reflect that during decade, though there is gradual increase in the incidences of crime, the crime rate specially under I. P.C., 1860 is gradually decreased. An analysis throws up new facets of crime and new ideas on how to cope with them. The real tragedy is that there is

---

2 See, Graph No. 1 on next Page No. 4.
hardly a national debate on the subject, like the ones seen in the United States and the United Kingdom.\(^3\)

**Graph No. 1**

The incidence & rate of crime for a decade from 1992-2002

![Graph of Incidence & rate of IPC crime](http://ncrb.nic.in/crime2004/home.htm)

Source: Crime in India, National Crime Records Bureau, New Delhi

### 1.3.2 Definition of crime: flagged by Socio-Eco-Political rider

Conceptual, crime is a relative phenomenon subjected to the relative socio-political & economical changes occurring in existing system of given society. Therefore neither all-time suitable comprehensive definition encompassing all aspects of 'crime' is possible at any moment of time nor can a single definition be made applicable to different society. Crime is a dynamic phenomenon. With its dynamicity, it is influenced by the changes occurs in the correlated phenomenon. In these days, money is more valuable than values. Incidentally economic crime is on its peak. This clearly reflects that crime has its interdependency with other social phenomenon.

---

Also, the population is one of the important factors influencing incident of crime. A positive correlation between the growth in incidence of crime and the population of the country has been observed. Besides population, the other factors influencing the crime situation at a particular place could be growing urbanization leading to migration of population from neighbouring place, unemployment, income inequality, [computer literacy in case of Cyber crime] etc.

1.3.3 Emergence of Cyber crime - origin is rooted in World War-II

The aftermath of World War-II has witnessed the drastic changes in every domain of life. The new mechanical adroit appear to convert all relationships of man with material things vanishing the boundaries between living and non-living being. Today mechanical adoption by human being is challenging the standards of conventional limitations laid down by time and space. The Cyber-technology has played major role in this transformation. The present study has been undertaken to touch some aspects, effect and prospects of this Cyber-technology with special reference to threat pose by Cyber crime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Commenting on the genesis of 'crime', Justice Sinha, Judge Supreme Court has quoted,

"Thus it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence. Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling over the society and it was always influence by religious-social-political-economical values prevailing in the given society. Thus from time immemorial the behavior that attracts 'penal liability' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes."

So far Indian society is concerned, particularly during ancient period, the definition of crime flagged by religious interpretation. The period was known for complete dominance of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period.

Gradually during medieval period, State started to emerge as independent entity by breaking of religious bondages. Marching on the line of secularism, State declared the socio-political and economical sphere as its sole jurisdiction and as crime fall in the list, the definition adopted to treat crime attempted on more secular principles. During this regime scientific and industrial revolution took place and State started to sponsor activities of venturing for new colonies.

Medieval period had evidenced the eras of renaissance and restoration, which delivered new, and a fresh look to ‘crime’. The concepts like utilitarian, positive approach, analytical thinking, principles of natural justice, and thoughts of lessie faire, hedonistic philosophy, and pain and pleasure theory were outcome of this period which helped to open new horizon for the study of crime. Latter period paved the way for scientific & industrial revolution and rational way of interpretation dominated the thinking.

This was the period when European countries hurled into wars for grabbing colonies in different parts of the globe. Incidentally, the legal system of various nations and different parts of the world started to merge and influence each other. This was the basic factor for defining ‘crime’ on more secular line having social and psychological riders. Historiographical developments of crime reflect addition and deletion of various acts as a crime and non-crime. Depending on the prevailing dominant factors, the list of criminal acts modified. During this period Indian Criminal System shaped by Britishers on colonial footings.

This process lasted long to World War - II when process of colonization not only stopped, but took reverse gear. Asian and African countries started to liberate from the iron pawn of continental countries to shape their own laws on domestic requirement. However, at the same time, neo-globalization process begins and new types of crime started to emerge challenging the age-old notion of sovereign and jurisdiction. These trans-national crimes overthrow the possibility of encompassing it
within domestic definition. One of such category of crime, which is new in origin, but requires treatment on different footing, is 'Cyber crime'.

1.3.4 Cyber crime - By-product of Computer Technology

In the information age the rapid development of computers, telecommunications and other technologies have led to the evolution of new forms of trans-national crime known as 'Cyber crime'. Cyber crime has no virtual boundaries and may affect every country in the world. Cyber crime may be defined as "any crime with the help of computer and telecommunication technology", with the purpose of influencing the functioning of computer or the computer systems.

Thus after World Wars, the fashion of grabbing of new territory and developing the colonies were come to an end. The manpower, techniques & tools, brains and intelligence that were earlier hurled into the development of new weapons, now turned their attention for using the technology for other purposes. Soon the result of using electronic technology appears on the scene. Telephone, radio, television, mobile phones, pagers, video games are some of the toys invented for the purpose. At the same time, the electronic technology has provided wider dimensions of its use in most of the sphere of life such as banking and financial sectors, accounting, calculations, visual presentations, digital libraries etc., The electron based technology emerge as an alternative for paper based culture. Thus at the end of second millennium and at the start of third millennium we feel to entering from printing culture to electronic culture where everything has been done with the help of computers, robots and adroit.

Speaking statistically, nearly one billion people around the world are now online. Worldwide Internet usage has grown by 146.2 % cent over the past five years. Seven Asia-Pacific nations are in the top 20 countries for numbers of Internet users, three China, Japan, and India - in the top five and Asia leads the world in the numbers of people now on the Internet with more than 300 million users, or 34 % of all the world's online users.6

1.3.5 Communication by Computer networking: Where the difference lies?

One of the characteristic features of modern way of communication is the varieties it provides. The options available with the communication and information

---

6 Quoted from 'Fact Sheet #2 IT use - World and Asia -Overview'. Published in 'Make-IT-Safe' official webpage www.make-IT-safe.net. Accessed on 25.02.2006 at 12.11.25.
dissemination through computer networking has its own limitations and leeway. It can be described in following words,

".... there is the matter of the differences between computer networks and other types of communication. The distinctive character of Internet communications for geographers comes from the Net's merging of three basic characteristics. First is a multidirectional interactivity: Any use can be a sender or a receiver. Second is instantaneity: Delay relate more to the speed of the processor used by the remote computer than to the distance of any browsed site. Third is transnationalism: Embargoing distant computer links is difficult without serving all outside telephone connections and thereby crippling economic development. Some of these characteristics may be shared with other media, such as the telephone and radio, but computer networks exhibit these characteristics to a unique degree. Furthermore, the World Wide Web provides a basis for multiple languages - textual, graphic, photographic, and cartographic - circulating at a transnational scale in a multidirectional and instantaneous manner."7

Thus, in this regards, the present technology adopted for communication and information sharing is much improved and deeply complex than other existing medias of communications and information sharing. Today, it is fast, speedy, multi-linguistic, storable, manipulative, or even, capable of challenging the age-old notions of time and space.

1.3.6 Why does Cyber crime dangerous and the deadliest crime?

One will wonder, at least, why is there growing importance of Cyber crime? Why does too much excitement about it? Why is the present day society treating it as deadliest forms of crime? And ultimately, why does too much hubbub there for protective mechanism? The answer is simple to reply and difficult to digest. Description of dangerous and the deadliest nature of Cyber crime can be seen from following paragraphs -

"Today we find ourselves dependent on pagers, cellphones, computers and electronic diaries and we wonder how we managed without them. The more dependency and the utility of them in day to day work have given birth to the darker side of internet age. Network crime[...] are the most unpredictable calamity on the Cyber world. Unauthorized access, hacking, spreading of viruses, smashing computer networks on very large scale, the brutal weapons like e-mail bombing, logic bombs resulting into the disrupt behavior of computer networks are very few incidences of recent days. This crime is high-tech and needs trained and equipped personnel to man investigatory and prosecuting agencies for effective prevention and control of computer related crime."

The difference between the pace of development of Computer Technology and efforts to safeguards society from its misuse and probable harm it may cause, the present situation is aggravated and worsens due to the computer illiteracy, resistance to adopt change, blunt response and lack of awareness in society. Today, technological transformation is happening across the world without any exception, but technological utilization, access, technological driving forces are in the hands of few.

The deadliest nature of Cyber crime can be put in the words of Vivek Sood, a famous legal thinker and expert who has commented -

"Cyber crime is the deadliest epidemic confronting our planet in this millennium. A Cyber criminal can destroy web sites and portals by hacking and planting viruses, play online frauds by transfer of funds from one corner of the globe to another and gain access to highly confidential and sensitive information. Moreover he can cause harassment by e-mail threats or obscene material, play tax frauds, indulge in Cyber pornography involving children, and commit innumerable other crimes on the Internet. It is said that none is secure in the Cyber world. The security is only for the present moment. With the growing use of the Internet, Cyber crime would affect us all, either directly or indirectly. Cyber crime such as hacking, planting computer

viruses and online financial frauds, have the potential of shaking economies. Cyber crime is presently estimated to be growing at the rate of 4.1% per week. From 640 criminal complaints (1.7 per day) in 1993 to the projected 2,82,000 (773 per day) for the year 2000, is not a slow journey by any standards. These are the figures when no more than 10% of Cyber crime gets reported.\textsuperscript{9}

In the light of above situation, Cyber crime seems to be the emerging trend of new criminality, which has potentiality to change the entire notion of set traditional road map of crime. Justice Sinha, Judge Supreme Court of India, while commenting on the nature of Cyber crime observed that -

"To understand Cyber crime as a significantly new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently effecting countries worldwide. This new technology not only provides opportunity for the profitable development of an international information market but has also raised the specter of new criminal activities to exploit them. They very technology that enables multinationals to do business more effectively and challenge the individual controls and regulations of nation states, also offers the prospect of globally organized criminal networks. Moreover the free flow of uncensored information on electronic networks and websites is an attractive to insurgents and extremist groups as it is to dissidents proclaiming their human rights."\textsuperscript{10}

Thus the advancement, inventions and revolution in the modern age are the basic driving factor for Cyber-technology. One basic difference between Cyber crime that demarcate it with traditional crimes is the sophisticated nature of criminals. The technology which is encircling around can be better understood by these sophisticated privileged class people. Again, most of the criminals learn the technology as a part of their curriculum.

\textsuperscript{9} http://www.tatamcgrawhill.com/digital_solutions/viveksood/chap2.htm  Accessed on 15.08.2005 at 24.11.2005

\textsuperscript{10} Sinha S.B., 'Cyber crime in the Information age.' Published in, 'Cyber Pace and the Law - Issues and Challenges' Edited by Ranbir Singh & Ghanshyam Singh, NALSAR University, 1\textsuperscript{st} Ed. (2004). PP. 1-2
Therefore, they are in better position to be acquainted with the technological adaptations as compare to those controlling machineries, which adopt technological knowledge as a part of their training programme at latter age.

While many efforts are underway to foster e-strategies for the development of new forms of electronic commerce and electronic government as well as host of other applications, the darker side of cyberspace is often shrouded in mystery or revealed only by the media as ‘moral panics’ over signs that the Internet is untrustworthiness or that the riskiness of cyberspace is substantial.\textsuperscript{11}

1.4 Ignorance of Cyber crime will be no excused

1.4.1 Cyber crime - Ignorance may prove fatal

Cyber crime is only important to a few people, but it should be important to everyone. If everyone becomes aware of the dangers of being online, the dangers will slowly disappear.\textsuperscript{12} It only if anybody tries to understand the potential harm the Cyber crime may cause can understand the danger of Cyber criminality. Computers, despite being such high technology devices, are extremely vulnerable. The description is not imaginary that to steal the national secrets from any government office or any information about military equipments from the computers of respective organization is comparatively more easily than to steal a loaf of bread from stall of unattained hawkers standing side by road. All over again, the risk involve the committing Cyber crime is very less due to its special characteristics.

Inquisitively, to be noted down, computers facilitate to such a great extend that one can imagine! For instance, it is difficult to filch a book, report, photographs or any other information in printed form from any house of office. But one can take it in the form of CD ROM where one can store lakhs of pages, thousands of photographs from any secure location. And if this secure place is connected to Internet, even theft can be completed via computer networking without being physically entering into premises. These make computer related crime more severe and serious now-a-day. Furthermore, as now a day the paper-based system


is rapidly replacing by electronic based system and more transactions are switching over to electronic format, the danger is growing ever fast.

1.4.2 What is Cyberspace where Cyber crime occurs?

First consider the word 'Cyber space'. What exactly it means? Indeed, in one sense, it is just a pattern of electrons skimming a net of computers, a construct that describes a location where a collection of activity occurs. But described like this, the space could not be understood, or at least it could not be understood by us. It is understood by us only when we put things into it, when we carry into it our own language, when we colonize it, when we domesticate it. It is no accident that we speak of e-mail, or that we describe postings on "electronic bulletin boards," or that we wonder about the dynamics of real-time discussions in "CB-chat" areas. We have no choice but to take control of this space at first with our ordinary terms, if indeed we are to understand it. And it is through a practice of analogy that this occupation occurs.

1.4.3 Cyber crime: the complex phenomenon - How so far to safeguard?

One problem with Cyber crime is its complexity to understand and safeguards. No doubt, computers are boon and it is very good servant as well having lot of potentiality. It works fast, effectively, efficiently, accurately, without taking pause, and continuously. It may not form any union, available twenty four hours a day, seven days in a week and without taking a pause for years together.

But after all computers works through programs specially design for the purpose. These programs are written in several lines compatible to computer readable language. These programs have some tips, instructions, processes and logic to be followed by operating systems. Operating systems are composed of millions of lines of code and no single individual can claim to understand the security implications of every bit of these computer instructions. The hackers are always in search of any lacuna or loopholes of this programming system. And if

---

they find it, they can break open the security of the programs and enter into the security zone where they can do any havoc.

"...[I]f anyhow the lacuna has detected and patched up, hackers can easily exploit the numerous weaknesses in operating system and security products. Thus when one weakness is exposed and exploited openly by the 'black hat' community, the operating system (OS) manufacturer patches it up. The hackers then find another weakness to exploit and the cycle goes on and on. It is far easier to find weaknesses in existing operating systems rather than designing and developing a secure operating system."

The basic question can be quoted here is 'does technology has any alternative? Or even more basic is 'why should technological adoption at all? It seems easy to discuss such issues but crises of technological adoption and analyzing alternative pose several complex problems. There is another aspect of compulsion for technological adoption. In the words of Alvin Toffler, a well known scholar in the branch of 'sociology of the future',

"Yet today we face an even more dangerous reality: many social ills are less the consequence of oppressive control than of oppressive lack of control. The horrifying truth is that, so far as much technology is concerned, no one is in charge.

So long as an industrializing nation is poor, it tends to welcome without argument any technical innovation that promises to improve economic output or material welfare. This is, in fact, a tacit technological policy, and it can make for extremely rapid economic growth. It is, however, a brutally unsophisticated policy, and as a result all kinds of new machines and processes are spewed into the society without regard for their secondary or long-range effects."

Graphical representation reflects that there is gradual and swift jump of digital production and consumption in India. The number of Internet user

---

15 http://Cybercrime.planetindia.net/Cybercrime_cell.htm Accessed on 15.08.2005 at 10.15.04.
16 Toffler Alvin, 'Future Shock', Daily express, PP. 388-389
increase by 800%. The following table will reflect the percolation and adoption of digital technology in India.

**Graph showing the Internet user subscribers in India for the period of 1998 to 2005**

<table>
<thead>
<tr>
<th>India: Internet Users and Subscribers: 1998 - 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Figures in thousands)</td>
</tr>
<tr>
<td>PC sales</td>
</tr>
<tr>
<td>280 880 1,030 1,403 1,682 2,083 2,228 2,764 2,953</td>
</tr>
<tr>
<td>Households</td>
</tr>
<tr>
<td>120 220 287 416 640 876 1,106 1,394 1,620</td>
</tr>
<tr>
<td>Businesses</td>
</tr>
<tr>
<td>660 810 1,136 1,656 1,554 1,700 2,125 2,763</td>
</tr>
<tr>
<td>PC population</td>
</tr>
<tr>
<td>1,170 2,130 2,810 3,764 5,970 6,709 6,802 10,480 13,486</td>
</tr>
<tr>
<td>Households</td>
</tr>
<tr>
<td>780 1,202 1,593 2,293 3,253 4,853 6,273 7,933 9,162</td>
</tr>
<tr>
<td>Businesses</td>
</tr>
<tr>
<td>4,290 5,304 6,789 8,155 10,385</td>
</tr>
<tr>
<td>Population (millions)</td>
</tr>
<tr>
<td>761 977 993 1,014 1,027 1,047 1,056 1,106 1,111</td>
</tr>
<tr>
<td>PC penetration (for 1,000 population)</td>
</tr>
<tr>
<td>1.18 1.27 1.28 1.32 1.44 1.49 1.82 1.91 1.92</td>
</tr>
<tr>
<td>Internet penetration</td>
</tr>
<tr>
<td>38 40 50 60 70 80 90 100 110</td>
</tr>
<tr>
<td>Households (percent)</td>
</tr>
<tr>
<td>60 80 100 120 140 160 180 200 220</td>
</tr>
<tr>
<td>Internet subscribers</td>
</tr>
<tr>
<td>25 130 330 530 1,130 1,763 3,561 4,403 6,674</td>
</tr>
<tr>
<td>Businesses</td>
</tr>
<tr>
<td>29 125 224 332 511 729 1,177 2,292 3,727</td>
</tr>
<tr>
<td>Households</td>
</tr>
<tr>
<td>10 50 100 150 200 250 300 350 400</td>
</tr>
<tr>
<td>Businesses (percent)</td>
</tr>
<tr>
<td>40 80 120 160 200 240 280 320 360</td>
</tr>
<tr>
<td>Households (percent)</td>
</tr>
<tr>
<td>10 20 30 40 50 60 70 80 90</td>
</tr>
<tr>
<td>User to subscriber ratio</td>
</tr>
<tr>
<td>30 11 12 13 14 15 16 17 18</td>
</tr>
<tr>
<td>Households</td>
</tr>
<tr>
<td>2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.5</td>
</tr>
<tr>
<td>Number of users</td>
</tr>
<tr>
<td>6,660 10,604 20,909 31,723 32,675 33,625 34,575 35,525 36,475</td>
</tr>
<tr>
<td>Businesses</td>
</tr>
<tr>
<td>5,114 8,124 15,649 23,951 24,905 25,859 26,813 27,767 28,721</td>
</tr>
<tr>
<td>Households</td>
</tr>
<tr>
<td>1,544 2,481 3,251 4,222 4,250</td>
</tr>
</tbody>
</table>

Source: NASSCOM

However, as these poor nations once start with adoption of technology either as policy for improving economic output or for gaining material welfare, the reversible process become hazardously difficult and situation goes out of control. Increasingly diverse innovations are arrayed before the society and the problems of selection grow more and more acute.

This requires serious attention for controlling and rational use of technology. As the prevalence of technological adoption by society increases, the nightmarish outcome gains plausibility. However, it is equally true that check and control of technology should not be detrimental to innovation and human creativity which is soul of change and transformation. Alvin Toffler has rightly commented,-
"The incipient worldwide movement for control of technology, however, must not be permitted to fall into the hands of irresponsible technophobes, nihilists and Rousseauian romantics. For the power of the technological drive is too great to be stopped by Luddite paroxysms. Worse yet, feckless attempt to halt technology will produce results quite as destructive as reckless attempts to advance it.

Caught between these twin perils, we desperately need a movement for responsible technology. We need a broad political grouping rationally committed to further scientific research and technological advance - but on a selective basis only. Instead of wasting its energies in denunciations of 'The Machine' or in negativistic criticism of the space programme, it should formulate a set of positive technological goals for the future."\(^{17}\)

1.5 Methodology adopted

Present study on the subject entitled, 'Legal Control of Cyber crime in India: Problems & Prospects' has its wide dimensions. As the Computer Technology has its origin in recent past, no much literature is available. Particularly, in the context of developing countries like India, the trend of using Computer Technology has encountered the initial resistance, and it take pace only in 90s decade. Incidentally, a Cyber crime appears somewhat new terms at Indian scenes.

Thus exploring the legal research in the area of Cyber crime by adopting legal approach encounter difficulties. First is the lack of literature, especially scarcity from Indian point of view has been experienced. Second, the Indian legal system has colonial impact and social perception for exploring research study is cynicism. Third, the pace of development of technology in recent time is too fast to coup up research study with it.

Again, it is acutely observed that in most of the developing nations like India, technology has to be adopted for keeping pace with economic competitions and enhancing gains in economic terms. However, the legal infrastructure to deal with its probable effect has always given a back seat. Therefore, in the legal infrastructure has always been weak and lagging behind in these country, though due to several contributing factors working for it.

\(^{17}\) Toffler Alvin, *Future Shock*, Daily express, PP. 389-400
1.5.1 Hypothesis

Hypothesis is a tentative statement(s) the validity of which is yet to be tested and an essential part of an research writing. It is the starting point to set a direction of research. The present study has been commenced with following hypothesis in mind.

i. **What are the various specialties of Cyber crime? What makes its specific categorization possible?**

In order to evaluate hypothesis, the attention has been paid to trace the specific nature of Cyber crime which demarcate the line of differentiation between traditional and this modern criminality. The attempt has been made to decide various parameters around this word 'Cyber crime'.

ii. **Can Cyber crime, so categorized, be really termed as 'Crime'?**

According to well-known legal maxim, *Nullum crime sine lege*, nothing is crime without prior declaration by law. It has been observed that there is acute difference between the definition of Cyber crime reflected in legal literature, and jurisprudential sense. Thus question may arise that if Cyber crime has not been defined, whether there is any point to consider it under the category of 'Crime'? however, none of the act which are otherwise harmful and capable to be declared as 'crime' under the act still left outside the purview of present legal literature. While evaluating present hypothesis, the attention has been made to decide whether Cyber crime can be really categorized as 'Crime'.

iii. **Why does Cyber crime need serious attention?**

The next hypothesis has risen about the need of serious attention. While attempt to evaluate the same, various dimensions has been analyzed. Various problems and prospects has been scrutinized.

iv. **What are the various difficulties in India for treatment against Cyber crime?**

As the research topic focus upon the legal control of Cyber crime in India, it is essential to check the legal response and its efficiency to control Cyber criminality, not only from Indian point of view, but in International perspective, because both incidences and impact of Cyber criminality is trans-national in nature. The technical aspects of controlling the cyber criminality with prevailing notions like national and sovereign has
been analyze, because, as the matter is directly correlated with legal system, which is a sole domain of national jurisdiction.

It has stressed upon to check various hurdles in combating this deadliest criminality. Definitely, it requires checking the legal, judicial, administrative level difficulties, as well as, as the Cyber crime is trans-national type of crime, to check national and international confrontations and consensus. A cursory glance has been given to the probability and prospective of future strategies, keeping human rights perspectives in the Cyberspace and framework in this regard. This brings national and international legislation and their study inevitable to be focus upon so that the Indian response to these deadliest types of criminality can be studies on more firm footings.

1.5.2 Basis presumptions

The present study has been undertaken with this mute notion that scientific study warranted the development of any branch. The methodology adopted is basically analytic type. However researcher has firm belief that the compartmentalization of these research methods is merely for the convenience and ultimate aim is to arrive at specific conclusion by developing specific theory and find out the sequence of facts occurs. Therefore, at the convenient place, the support of other methods has been taken. Ultimately, it is research knowledge, which is more important that technicality and preference always has been given to prior over latter.

Researcher has firm belief that though ultimate truth is difficult to achieve, one can attempt to go nearby. It has been tried to retain objectivity during research, and efforts has been made to avoid subjectivity, however, it would be the sole domain on scrutinizer and reader to judge how so far the researcher is successful in achieving in the objectivity and objects.

1.6 Conclusion

Thus it is quite clear that to understand the word 'crime' in its general connotation and 'Cyber crime' in particular, socio-economic & political enquiry is inevitable. Again, as Cyber crime is a by-product of Computer Technology and its growing use for Information & Communication, all those factors that are influencing the modern trends are essentially scrutinize. Again to make the study more relevant, we have to understand to the zone where various interests are conflicting with each other. Thus, individual interest for use of available technology, national interest to
secure its community from inner and outer threat, sovereign privilege of non-interference of any extra-territorial authority, trade and developmental thrust are major consideration in the area of Cyberspace. However, it is sure, that evolution is irreversible process and we cannot step back from it. What remain in our hand is to change the direction of progress, and we stick up to our commitment to turn it in the direction of sustainable development. Thus, it is a high time, rather overdue to think and plan over the issues like Cyber-crime to remain secure in Cyberspace.

It is observed that in India 'Technological Adoptions' are matter of reputation or envy but not necessity. Why do we purchase TV? Mobiles? Computers? Pagers? Most of the times because of our neighbours are having it!!! Why do we gift Video Games to kids? Because it is a trend! But do we have thoughtful consideration of its utility, necessity and justification?

The 'Technological Adoption' should be scrutinized and introspected with 'Domestic Justification', particularly for developing and underdeveloped community where compelling priority and developmental level differ from western countries. The developed countries are abundant in recourses, but not developing and underdeveloped one! Therefore these nations are struggling hard to balance between their recourses and requirements. Technology can be the recourses, but the country like Indian should think over its justification before adaptation. This is a time to act, to plan, to get protected the generation, because electronic technology has greater potentiality to destroy society than any other previous variables. The threat is more dangerous than even before. Surely, if we fail to plan, we plan to fail!