INTRODUCTION

From the beginning of the civilization there has existed some mode of communication. As the civilization developed these modes of communication also changed. A human being always strives for better comfort or convenience and inventing and adopting new modes of communications is no exception to it. The subject matter of any legal studies is pertaining to law. In as much as, law, in some form or other has existed since human beings first associated themselves in settled communities, it is clear that there has been continuous examination of the nature and function law.

Such a process is an elementary founding stone to the practice of law at any rate in a developed society. Thus as the civilization developed, man has constantly adapted himself with the changing circumstances and scenarios to usher in new eras of development and progress. Every stage of human history has been important in its own way. However, if today we think in retrospect and try to analyze the pace of various important advances, some periods stand out.

As the civilization enters into the new millennium, technology has suddenly taken a new meaning. The world is undergoing a technological revolution. This revolution has created new complex legal problems, over which no government is able to exercise complete control. As the human civilization develops new questions and problems crop-up. In welfare state it is never expected that law should be static. It has to change with the change and development of the society. But this change is not an overnight process. It is a gradual process of metamorphosis, and law must keep pace with these changing needs of the society. Law must respond to the cry of the community and it must be ready to serve the needs of the society. New problems ask for new solutions and to resolve such problems law must be flexible enough. Old, rigid and outdated laws have no place in developing societies.

With the advent of "INTERNET" the world has become a global village, whereby present law enforcement machinery may not be adequate to satisfy the needs. The Internet had its beginnings in the late 1940s at the US Department of Defense during Cold War where the main aim was to maintain communications in the event of nuclear attack. The Department of Defense established the Advanced Research Projects Agency (ARPA), which created ARPAnet, the embryonic Internet. ARPAnet was used to connect vital US military and research sites. Because the computers at these sites were of different types, ARPA developed a common language, or protocol, that enabled secure communication among them. In the late 1980s, the National Science Foundation (NSF) began expanding its own network, NSFnet, with the goal of allowing access to educational and national research institutions for exchange of e-mail, files and data. Based on ARPAnet technology and protocols, NSFnet evolved to connect with other TCP/IP networks around the world, to allow open, public participation, and to be called Internet. Commercial use of the Internet began to grow slowly in the early 1990s and then virtually exploded as corporations came to realize the Internet's value for promotions, public relations, information dissemination, and the beginnings of electronic commerce. Information sent via net is broken into bites and these bites will

select its own route to reach the destination. Finally they will get together at the destination. Thus net is decentralized..i.e. no human agency regulates the way the information travels.

In the last decade the human civilization has witnessed a significant technological transformation. It is felt that law must have a universal quality in the present era in its application. The explosion of new and pertinent statutory laws over the past two decades reflect society's attempt to wrestle with an ancient phenomenon in a modern context. Wrongs of all sorts occur all the times, and the individuals, organizations and legal machinery try to address them in all possible ways.

The dawn of the new millennium has given us a new mode of communication. The information superhighway is undergoing a rapid growth. The Internet and other telecommunication technologies are promoting advances in virtually every aspects of society and every corner of the globe fostering commerce, improving education and health care, promoting participatory democracy in Indian and other countries, and facilitating communications among family, friends, whether across the streets or around the world. The Internet is re-defining the relationships and transforming the lives in such a way that the communication will never be the same again. With the Internet, one can communicate at the click of the mouse to the nook and corner of the world. Immediacies and interactivity are the key words of Internet revolution.

Unfortunately, many of the attributes of modern technology such as low cost, ease of use, and anonymous nature, etc.- make it an attractive medium for fraudulent scams, child sexual exploitation, website hacking, introducing viruses, and so on.... Conventional law, which provides dispute resolution machinery, fails in this 'CYBER JUNGLE'. Internet is re-wiring our relationships and the life is never going to be the same again. This advent of global computer network has rendered geographic boundaries increasingly porous and ephemeral. As digital technology has advanced over the past 50 odd years with a force unprecedented in history, governments, business and people around the world have been affected immeasurably. The already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary data changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of earlier generations.

It goes without saying that the aforesaid new technological developments have conferred substantial benefits. However, fundamental restructuring of society also results in certain disadvantages at all levels. Our vulnerability increases with the perceived value of and reliance on this technology. Increased opportunities for the industrious to be more productive also allow the less-upright avenues for malevolence...Internet which is the cheapest and the fastest mode of communication has brought with it a new name of crime, called cyber crime. In the information age the rapid development of computers, telecommunications and other technologies have led to the evolution of new forms of trans-national crimes known as **"cyber crimes".** Cyber crimes have virtually no boundaries and may affect every country in the world. They 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.

Laws develop in response to society's needs. They evolve in the context of the culture, business practices and contemporary technologies. The law currently governing commercial transactions were largely developed at a time when telegraphs and typewriters were commonly used, office technologies and business was conducted with paper documents and through mail. Technologies and business practices have dramatically changed but the law has been slower to adopt. Computers, electronic networks and information systems are now used to process, store and transmit digital data in commercial field. As the spread and use of information technologies in the business world have quickened, inadequacies and deficiencies of the current laws to meet the needs of digital, information-based society have become apparent. Electronic commerce has opened a new way of doing business. A variety of new challenges have come up for those who use Internet for business purposes.

A new stream of law – **Cyber law** - has emerged. Cyber law refers to the legal issues that arise within the newly emerging area that is increasingly becoming known as cyberspace. More specifically, it relates to the interaction of law with information communications technologies and computer mediated communications systems. It, therefore, has a different agenda to that of either computer law or the law of the Internet, which, respectively, often show little difference from the law relating to contract or patents, or publishing or broadcasting law. Cyber law nevertheless has a separate identity. The distinctions among the three relate not just to subject areas but, importantly, to the qualitatively different levels with which each engage with the study of law. Cyber law exists at the (cutting) edge of law, where the ability of existing law to achieve its goals is challenged. In this sense the "law" in Cyber law is a much broader concept, it is "law in action" as opposed to "law in books" as it applies to situations where Law cannot cope. It therefore takes as its subject the wider range of regulatory responses and strategies of governance that subsequently arise. Activities in cyberspace have influenced many branches of law, like Commercial law, Intellectual Property law, and Evidence law. Unique situations, created by the tremendous growth of the Internet usage, have to be addressed in Cyber law. While legal systems of different countries are grappling with the questions of developing Cyber law by applying law or through innovations designed to meet the novel challenges (especially problem of jurisdiction) posed by the Internet, time alone can tell whether the progress will be adequate to meet the evolving business needs of the global community.... It remains to be seen whether the current approaches to deter and redress computer crime will prove successful. Naturally, Case law has been slow to develop. Most likely, it is still in a nascent wave of inevitable prosecutions. All elements of law enforcement are themselves – by and large – in infant stage.

SIGNIFICANCE OF THE STUDY

Much has been said about the coming of the Internet and how it contributes to and detracts from our lives. A prime concern as we stand on the threshold of life in the Internet age is the role it will play in the perpetration of crime.

The Internet, together with other telecommunications wonders, has turned the world into a global village. It has eased and expedited the pace of communication and interaction among business communities, consumers, government agencies and society in general by removing traditional middlemen links and cutting through unnecessary red tape. This enhances overall efficiency and results in increased productivity in all sectors of the economy.

The technology that has spurred the growth of the Internet is still changing at an expedient rate and the traditional paradigm that the world is used to in managing its affairs has been changed irreversibly. Unfortunately, like all previous inventions of mankind, Internet technology can be used for both good and evil purposes. In the wrong hands, it will facilitate the commission of all traditional criminal activities and spawn a whole new series of criminal activities called cybercrimes, which the world may be ill equipped to cope with, if the problem is not nipped in the bud. Society is facing a new name of crime called cyber crime. A name, which was unheard, has now become a part of our lives.

The significance of the study lies in the fact that Internet, which is decentralised mode of communication has given birth to the new form of crime called cyber crime. The researcher via his work tries analyze what kind of jurisdiction problems the courts have to face while resolving disputes relating to cyber crimes. Society is facing crimes like Hacking, Launching virus, Password sniffing, Cyber stalking, Internet gambling, Spamming, Software piracy etc. What has become a worst nightmare is the then law enforcing machinery fails in this cyber jungle. The moot question that has troubled almost all the nations is – 'which court has jurisdiction to resolve Internet disputes'.

Use of Cyberspace is a unique and entirely new means of mass communications that is located in no specific geographical location and yet is accessible to anyone, anywhere, who has availability to it through computer link to the Internet. Consequently, there is no single organization or nation that controls membership in this virtual land, nor is there a centralized location from which access is regulated. These features of Internet make it different from other means of communication.

The decentralized nature of the Internet poses challenging problems for the terrestrially bound government and individuals that have an interest in the real injury generated through the use of this "unregulated" medium. Since no single government controls the citizenship of Cyberspace it opens up a green ground for criminals for committing conventional crimes (also cyber crimes) via new mode of technology. Jurisdiction is the power of the court to decide the disputes between the parties. Without jurisdiction, the judgment of the court would be of no value. Internet has vanished the geographical boundaries, which use to play significant role in deciding disputes. On-line transaction has given rise to novel

question of 'Jurisdiction'. The Internet permits netizen to interact and transact with one another across geographical boundaries with luxurious ease.

The researcher in this work has attempted to answer these burning issues as to which court has a jurisdiction to resolve the disputes when there is crime via Internet. It is found that Conventional law enforcement machinery is not applicable becoze Internet has no geographical boundaries. The question that arises is which court has a jurisdiction to resolve the dispute when there arises a conflict of law situation. It is quite obvious that when there will be cross-border transaction there are bound to be conflicts of law situations. The situation becomes more difficult when the transactions are done through Internet, which doesn't respect nations boundaries. Attempts are made at both national and international levels to answer these questions.

The ability of the Internet to reach across borders has raised a host of questions, including questions of legal jurisdiction. Should defendants be haled to a jurisdiction where, though their websites are accessible, they had no intent to do business? Several recent court decisions on interstate jurisdiction point to the beginnings of a standard for determining whether an entity has "purposefully" directed itself to Internet users in another jurisdiction. At the international level, the disparate legal approaches between countries magnify the potential problems. The Internet has created many challenging legal issues for the courts, not the least of which is the question of jurisdiction (the power to hear a case). The Internet can allow computer users anywhere in the world to search and retrieve information from a publicly available site anywhere else in the world. Although this potential global audience can mean great exposure for businesses, it can also translate into potential liability.

The significance of the research work lies in the fact that this study tries to focus on the most burning problem of the world as on today's date. The study focuses on problems like which courts have jurisdiction to resolve on-line disputes involving conflict of law situation. Further the work focuses on the question as to how cyber crime is different from conventional crimes. Also in-depth analysis is made as to how Internet works and what makes it decentralized mode of communication. The researcher has made a critical study of the IT Act and also focused on some of the lacunas in the Act. A comparative study of jurisdictional principles of the U.S. and Canadian law is also done. Extensive study of the case laws has been made. The decisions given by US courts have been analyzed from Indian perspective. Study is also done in the cases where the courts have given divergent opinions though the facts of the cases were similar. After going through the laws of the USA and Canada a comparative study is done with IT Act 2000. Also in depth analyze of the recent Internet related case laws has been done.

OBJECTIVE OF THE STUDY

Cross border transactions are becoming common and therefore Internet contracts have given rise to conflicts of law situation. Different countries are having different laws and therefore at times it becomes difficult to tackle the disputed problems.

The study centers round the problem of jurisdiction, which the disputing parties have to face when they had cross-border transaction via Internet. Conventional law works on the premise of geographical boundaries, which is not applicable to Internet. What exactly are 'cybercrimes'? In loose terms, they refer to any criminal activities that are facilitated by or committed by the use of or against a computer. Under this broad definition, cybercrimes are viewed as a sub-set or an extension of the generic term 'crime' and anybody who uses a computer has the potential to become a cyber criminal. For example, a traditional criminal, such as an unlicensed gambling racketeer, may be re-classified as a cyber criminal if he sets up websites offering online gambling in addition to his gambling dens. However, the criminal laws outlawing gambling will apply across the board, irrespective of the virtual mode of operation for the purposes of imposing criminal liability.

Some believe that cybercrimes is a separate and distinct phenomenon from traditional crime with material differences that require a new approach in the imposition of criminal liability. Underlying this belief is the perception that virtual crimes are actions in cyberspace, i.e. a shared virtual community that is fundamentally different from crimes committed in the physical world. As such, the application and standards of criminal laws for the virtual community should be markedly different from those commonly applied in the courts of the physical world. Though appearing far-fetched at this point in time, the consequences of adopting this view are that it will result in the creation of cyber courts administering, perhaps, cyber justice.

Be that as it may, the harm suffered by individuals or corporations arising from cybercrimes are real and can be proven in court. Often, cybercrimes extend beyond national borders and involve the laws and people of different nations. This makes their detection all the more tedious, especially when investigative agencies of the respective countries are not co-ordinated in their field operations and are caught in a quagmire of multiple jurisdictional and conflict of laws issues. Accordingly, it is imperative that our laws and enforcement agencies keep up with technological development and form international alliances to curb this global menace.

The object of the study is to focus on following issues:

-Whose jurisdiction is there in cyberspace?
-Which nations laws are to be applicable when there arises conflicts of law situation?
-What are the problems that the law enforcement machinery has to face while enforcing the principles of jurisdiction?
-Can we apply the old rules of jurisdiction to Internet?
-A study of provisions relating to jurisdiction in Information Technology Act 2000.
-Comparison of basis of jurisdiction in the USA and Canada with IT Act 2000 with detail study of case law.
-To recommend necessary amendments in IT Act 2000
-To study various approaches that has been adopted by the USA, Canada and India to regulate Internet.
-Various Cyber crimes and legal provisions to curb the same

~~Hypo~~ HYPOTHESIS FORMULATED

~~METHODOLOGY ADOPTED~~

Since cybercrimes cross multiple jurisdictions, the obvious difficulty in any legislation enacted to regulate conduct in cyberspace is empowering domestic courts with the right to hear cases on crimes committed in foreign countries and involving international personalities.

For example, the state prosecutor of a country will have to consider the issue of whether foreign operators of a website situated in cyberspace or in another country that offers online illegal activities, such as gambling and pornography, may be prosecuted in the former country that outlawed gambling and pornography. This is important when these foreign operators target members of the prosecuting country as the consumers of the services offered by their websites. A negative answer will impair the ability of the prosecuting state to control or regulate the prohibited activities in its own country. This is because the perpetrators of such activities could avoid criminal liability simply by operating their website out of jurisdiction. More complications arise when the laws in the countries in which these foreign operators operate from recognise the online activities as legal, e.g. online gambling and adult sites may well be legal in certain states in the US and Australia. The issue then is the status of the actions of such individuals as far as the laws of those countries, which outlawed those activities, are concerned. Can these persons be arrested for having committed an offence in the other countries when they step foot there? Likewise, can operators of certain websites in Singapore containing politically or religiously sensitive materials be incarcerated in neighboring countries where such sites are outlawed, assuming their cyber laws have extraterritorial effect? Whatever the answer may be, one thing is certain: steps will have to be taken to evolve universally accepted laws to govern cyberspace in order to avoid an absurd situation whereby the legality of virtual acts are determined by the location of commission, which would be totally inconsistent with the borderless realm of cyberspace.

Apart from jurisdictional difficulties, the enforcement of cyber laws are equally, if not more, problematic. Enforcement agencies, which do not have adequate technical knowledge, will be hampered in their attempt to complete the evidentiary link between cybercrimes and the cyber criminal. More sophisticated cybercriminals will be able to erase all evidence of wrong doings or make their detection impossible by logging into websites under the cloak of anonymity or by impersonating somebody else or by simply rerouting their logged on paths through a convoluted web of servers circulating through several countries before hitting the computers of their victims, who may be their colleagues sitting at the next table. The improbability of the detection of cybercrimes is a very serious problem because it attacks the very pillars on which the Rule of Law stands. If the perpetrator of a cybercrime can go undetected on the basis of his superior technological knowledge, then the law will lose its bite and there will be anarchy in cyberspace. By reason thereof, some have argued for the proposition that the relevant authorities must be given the technological edge in dealing with cybercriminals, including the leeway to 'tap' or secretly hack into the computers of suspected cybercriminals in the same manner that telephone lines of suspected criminals are monitored, in aiding the policing of cyberspace for the larger interest and the common good of the virtual community.

Some important hypothesis has been formulated to conduct the study. They are as follows:

- Internet, which is the latest mode of communication, does not consider geographical boundaries. Cross border transactions between the parties via - - -
- Internet has given rise to a novel problem of jurisdiction and conflict of law situation.
- Internet is decentralized media and it is not possible to regulate the contents available through it.
- Different nations are having different laws and therefore it becomes more difficult to regulate the net. Moreover there is also a difference in the moral standards among the nations which gives rise to hurdles to regulate the net.
- Basis of jurisdictions are vague in some nations and therefore there is no consistency in the jurisdictional principles.
- Law enforcement becomes more difficult as Internet is decentralized mode of communication. Conventional law enforcement machinery fails in this cyber jungle.
- Legislations enacted to answer the jurisdictional problem are very general in form. At times they fail to answer specific problems like IPR theft, Cyber stalking etc.

METHODOLOGY ADOPTED

As the duty is both technological and legal in nature, it is not possible to study these aspects by experimental method and hence Doctrinal Method is adopted for the study.

To conduct the study, the relevant information is collected from the specific and related enactments, various rules prescribed by both private and governmental

agencies and related conventions and treaties at the National and International level. The study also deals with various Rules and Doctrines evolved by the judiciary in specific cases. The area of law is still in its initial and developing stage and therefore it is required to rely heavily on the primary and secondary sources from which the relevant material is collected to conduct the study. The material and information are collected from sources like various relevant statutes, published books, published works, National and International journals, paper presented at National and International seminars, symposia, conference and workshops, original judgments of various National and International courts and relevant web-sites available on the topic.The study also includes a comparative analysis made of various national and international legislations on the subject. An effort has been made to compare and contrast the analysis drawn from the views expressed by such agencies that are at the helm of affairs.

REVIEW OF THE CHAPTERS

The study reviews the complexities and uncertainties surrounding the impact of jurisdictional aspects of cyber crime. Keeping this in view the researcher has divided the study on seven chapters dealing with different dimensions of the problem.

First chapter, which deals with the introduction part, has been divided into two parts. Part first covers law and its growth, modes of communication that mankind has witnessed and how it has influenced our lifestyles. It further discusses as to how Internet has changed the way we communicate and what are the advantages that society gains due to Internet use. Part two deals with nature of Internet, its birth and history. Further it also discusses in detail about the decentralized nature of the Internet and how it becomes difficult to regulate the Internet. Before going to second chapter, part two of first chapter deals in brief as to what is cyber crime and what laws are there to combat the cyber crime.

Chapter two of the study exclusively deals with the Information Technology Act 2000. It focuses in detail the important provisions of the IT Act. It also discusses in detail as to what are the offences covered in the Act. It also discusses the definition and kinds of cyber crimes in brief. Further the researcher has also pointed out the lacunas in the Act and made certain suggestions for amendments.

Chapter three is very part of the whole study. It deals with the darker side of the Internet. It covers in detail as to what makes cyber crimes different from the conventional crimes. It discusses in detail as to what is cyber crimes and different kinds of cyber crimes. A detail study as to cyber pornography is covered.

Chapter four exclusively deals with Internet Pornography. Initially it tries to define the terms 'obscenity' and 'pornography'. Then there is a comparison of S.292 of IPC and S.67 of the IT Act. At attempt is made to comment on how

Internet pornography is more harmful to society then conventional way of availability of pornographic material. Detail study of case laws has been done. The chapter also discussed what measures are taken by USA and Canada to regulate the pornographic content. Further an attempt is made to suggest ways and means may be adopted so as to regulate the availability of the Pornographic content on the net.

Chapter five is the core part of the research work. It exclusively deals with the issue of Jurisdiction, its evolution, and kinds. Initially it starts with the basis of civil and criminal jurisdiction of Indian courts. Then it deals with the question whether these principles of jurisdiction applies to Internet. It also discusses in detail the pros and cons of jurisdiction provisions in the IT Act. The chapter goes further to discuss in detail the jurisdictional provisions of USA and Canada and comparative study is made.

Chapter six deals with right of privacy in digital age. In it various aspects of privacy and how right to privacy is affected is discussed. It also discusses ways to protect the right of privacy.

Chapter seven deals with different measures that have been taken by USA and Canada to deal with the menace of cyber crimes. The chapter also deals with the issue whether those measures are adequate.

Chapter eight deals with conclusions and suggestions.

CHAPTER 1: INTRODUCTION

1. INTRODUCTION

The subject matter of any legal studies is concerned with various aspects of law. In as much as, laws, in some form or another have existed since the human civilization first associated itself in settled communities, it is clear, that there has been continuous examination of the functions and nature of law.

Such a process is an elementary founding stone to the practice of law at any rate in a developing society. Thus, as the civilization develops, man has to constantly adapt himself to the changing circumstances. Every stage of human history has been important in its own way. However, if today we look back in retrospect and try to analyze the pace of various important advances, some periods stand out. As the civilization enters into the new millennium, the words of 19th century have suddenly taken a new meaning. The world is undergoing a remarkable technological change. This change is creating complex social, economical, and also legal challenges over which no government, even of the most advance nations, is able to exercise complete control.

As the human civilization develops, new questions and problems crops up. In Democracy it is never expected that law should remain static. It has to change with the changing needs. But this change is not an overnight process. It is a gradual process of metamorphosis, and law must keep pace with these changing needs of the society. Law must respond to the cry of the community that it is there to serve the needs of the people. New problems and questions ask for new solutions and to resolve such problems law must be flexible enough to meet the ends of justice. Now with the advent of technology the world has become a 'global village' whereby present law enforcement machinery may not be adequate to deal with the new challenges. In the last two decades the human civilization has witnessed a significant technological change. It is felt that law must have a universal quality in the present era in its application. The

explosion of new and pertinent statutory laws over the past two decades reflect society's attempt to wrestle with an ancient phenomenon in a modern context. Offences of all sorts occur all the time, and the individuals, organizations and legal machinery try to deal with them, and seek new remedies.

2. LAW AND ITS GROWTH

"The history of law is the history of civilization, and law itself is only the blessed tie that binds human society together. ... Our long armed and hairy ancestors had no idea of redress beyond vengeance, or of justice beyond mere individual reprisal. The law, like everything we do and like everything we say, is a heritage from the past."

(John Marshall Gest, "The Law and Lawyers of Honoré de Balzac," The Lawyers in Literature (Boston: The Boston Book Co., 1913) at pp. 115,200,232)

Historically, law evolved by way of social customs, which was accepted by the society even before the legislation came into force. Voluntary forms of governance through customary private laws pre-existed state law and effectively ordered human affairs. Law arose as a spontaneous order – something to be discovered rather than enacted. Law is an evolutionary systemic process involving the experiences of a large number of people.

The idea of law includes fundamental rules of behavior, as well as institutions and devices for changing, clarifying, refining, and applying the rules. Law is a natural outcome of people living and working together. If people are to live with others in a society, there must be a way to resolve the inevitable disputes. Law can be seen as an instrument of subjecting human conduct to the governance of rules. The evolution of the law can be found even before rules were codified. It has also its roots in judicial decisions. In fact, the development of rules in society predates both courts and the written law. For thousands of years, customary and private legal systems alone ordered human activities. The power of customary law is found in the fact that it is reflected in the conduct of people towards one another. The more a society moves away from customary and

private law systems, the greater the need for laws coercively enforced by the state arises. Thus, law is essentially discovered, and not made. It is a systemic discovery process involving the historical experiences of successive generations. It reflects and embodies the experiences of all men who have ever lived.

Enormous scientific and intellectual advancements took place in the 17th century, and the Enlightenment, -- the Age of Reason was brought about in Western Thought, the age of the scientific man. The thinkers of the age were no longer content to accept the cosmos and its contained life as a mystery to be simply accepted. The time had come for man to test his theories which flooded into his mind; to test these theories with his observations and to reset these theories in accordance with his accumulated observations: and, seemingly without end, to continue to retest and to reset.
(See: Law – www.bluepet.com/Literature/Essays.htm)

From wheels to aircrafts, and from stove to microwave ovens, technology has played very important role in our life. We are getting more and more dependent on the computer for our daily affairs.

Now with the advent of the Technology and Globalization the fundamental concepts of Law are required to be changed. It is now felt that rapid growth is in need of swift responses. It is rightly said, " Law behaves like a traditional Hindu wife staying seven steps behind her husband". The outburst of new technological advancement asks for the new mechanism to resolve new form of disputes. There is a gradual shift to paperless world and this requires our law enforcement machinery to be on the cutting edge. Thus the growth of the technology marks for the development of the mankind too. But at the same time, there are new forms of disputes, which the civilization had to face. The law must be flexible to meet those needs. With the growth of technology there arises new problems and law must keep pace with the new issues. 19th century has brought along with it new colors of crimes with sharp technological edges. What has been witnessed by the present civilization is that, fundamental concepts of law require a re-orientation - of both basic ideas and presentations as well. The definition of law, that 'it is an ideal course of human conduct' is

gaining a slow shift. New kinds of Hi-tech crimes requires, the law givers and interpretators to have that technological intellect, both, to understand and to combat the menace of INTERNET CRIMES.

The emergence of global digital networks, such as the Internet, and digital technologies that enhance human abilities to access, store, manipulate, and transmit vast amounts of information has brought with it a host of new legal issues, which 21st century would be required to address. Although many nations are trying to map existing legal concepts with problems arising in cyberspace, it is becoming increasingly evident that this strategy sometimes doesn't work. In some cases, it is necessary to go back to first principles to understand how to accomplish the purposes of existing law in digital network environments.

Globalization And Emergence Of The Digital Network

Many of the traditional jurisprudential notions and percepts that are being taught today have become outdated. Today the whole thing requires an entire overhaul. The law of a country cannot afford to be entirely exotic, for the simple reason, that law in its ultimate analysis remains the relative expression of the life and the spirit of the land and the community it serves. Law must have universal quality in the global age. Law is the "Alphabet of globalization" and it should not demonstrate political bias of the party concern. The new forces, vast commercial industrial and technological expansion, the rise and growth of mental and physical science and their application to life, the changing theories of technological advancement and many other social and economic development requires apparently a new platform for up-coming legislation to answer new questions. The world emerging out of new technology and science opens a wide vista for hi-tech criminals.

The information superhighway is undergoing a rapid growth. The Internet and other telecommunication technologies are promoting advances in virtually every aspects of society and every corner of the globe fostering commerce, improving education and health care, promoting participatory democracy in Indian and other countries, and facilitating communications among family, friends, whether

across the street or around the globe. Explosion in the Information Technology has paved a way to 'INTERNET'.

The Internet is re-defining the relationships and transferring the lives in such a way that the communication will never be the same again. With the Internet, one can communicate at the *'click of the mouse'* to the nook and corner of the word. Immediacy and the interactivity are the key words of Internet revolution. Unfortunately, many of the attributes of this technology – low cost, ease of use, and anonymous nature among others – make it an attractive medium for fraudulent scams, child sexual exploitation, website hacking, introducing viruses, and many more. Conventional law machinery has failed to combat the new forms of crimes called Cyber crimes. Internet is re-wiring our relationships and the life is never going to be the same again. This advent of global computer network has completely disregarded geographic boundaries. As digital technology has advanced over the past 50 odd years with a force unprecedented in history, governments, business and people around the world have been affected immeasurably. The already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary date changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of the earlier generations.

Laws develop in response to society's needs. They evolve in the context of the culture, business practices and contemporary technologies. The law currently governing commercial transactions were developed at a time when telegraphs and typewriters were commonly used, office technologies and business was conducted with paper documents and by mail. Technologies and business practices have dramatically changed but the law has been slower to adopt.

Computers, electronic networks and information systems are now used to process, store and transmit digital data in commercial field. As the spread and use of information technologies in the business have increased, the failure of current laws to meet the needs of a digital information based society has become apparent. Electronic commerce has opened a new way of doing

business. A variety of new challenges have come up for those who use Internet for business purposes. A new stream of law – Cyber law has emerged. Activities in cyberspace have influenced almost all branches of law, like, Commercial law, Intellectual Property law, and Evidence law etc.

Unique situations, which have been created due to the tremendous growth of the Internet usage, have to be address by Cyber law. While legal systems of different countries are grappling with the questions of Cyber crimes, by applying traditional law, time alone will tell whether these traditional principles of law will be adequate to meet the evolving legal issues. It remains to be seen whether the current approaches to deter and redress computer crime will prove successful. Case law has been slow to develop. Most likely, it is still in a nascent wave of inevitable prosecutions. All elements of law enforcement are themselves – by and large – early in developing an understanding of the nature of these offences and how best to enforce the law.

The explosion of new statutory laws shows how different nations are trying to answer the new disputes. Wrongs of all sorts occur all the time and law enforcement machinery tries to address them, if at all, possible. But only sovereign can take a persons life and liberty, and then only after due process of law to address the commission of crimes which a legislature has specified in advance. Thus all the inequities which significantly involve or revolve around a computer, only those labeled as crimes mark the limits of behavior beyond which certain civil rights of perpetrator are subject to forfeiture coupled with the fascinations of our Information age, the world of criminal justice provides an interesting vantage point to access how our complex community tries to restraint itself while racing into the future.

The Internet has changed the way we communicate and it has revolutionized the global market place. Products and services once offered only at the local store are now available to consumers at every corner of the planet. Thousands of traditional brick-and-mortar stores are taking their business on-line, hoping to stake their claim to Internet fortunes. Millions of individuals, in every corner of globe are logging to net each day to seek information, communicating ideas,

and transacting business. This prolific growth is fuelled by the relative ease of transmitting information nationwide or worldwide, instantly. Easy of use, powerful and effective communications that are interactive and in many instances occur in real-time and a culture that encourages the use of computers has created the "virtual storefront".

Each minute, over five million e-mail messages are now being sent around the world. While it took more than a century to install the first 700 million telephone lines, the next 700 million will be installed in less than 15 years – 300 million in China and India alone. In the same period, there will be 700 million new wireless subscribers. It is forecast that there will be 1000 new communication services providers worldwide within the next two years [1]. In recent years, the number of computers and users connected to the Internet has skyrocketed as well. The number of computers hooked up to the Internet globally in 1992 totaled only 1.3 billion [2], whereas currently there are more than 68 million worldwide [3]. Today, there are nearly 260 million users internationally with Internet access [4] and forecasts projects there will be over 765 million users by 2005 [5]. In Europe, Internet users in 2000 climbed to nearly 135 million, the Asia-Pacific region reached upto 73 million, while South and Central America climbed 24 million [6]. Undoubtedly, the Internet has redefined the way we communicate.

The beauty if the Internet is that, it breaks the data into bytes and these bytes will take up their own route to reach to the destination. The Internet is a rare example of a true, modern, functional anarchy. There is no "Internet Inc." There are no official censors, no bosses, no board of directors, and no stockholders. In principle, any node can speak as a peer to any other node, as long as it obeys the rules of the TCP/IP protocols [7], which are strictly technical, not social or political. As compared with other modes of communications there can be some regulation that can be imposed. For example, the content provided via television and movies can be censored through censored board. Again, one can make out who has launched that particular content, and from where. In case of Internet, there are no such provisions. One cannot make out from where the content is launched, and again if it is known, you cannot enforce the

legal provisions of your land, becoze law changes from land to land. Again when a person logs on through the net he can successfully hide his/her identity. This provides green ground for the wrongdoers to commit crimes swiftly.

3. THE TERM 'INTERNET' DEFINED

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. To develop proper analysis of the issues surrounding the Internet cases, an understanding of the Internet and its working is required.

To start with, Internet is not a physical or tangible entity, but rather a giant network, which interconnects innumerable smaller groups of linked computer networks. (ACLU v Reno 929 F Supp. 824 www.bna.com/e-law/csese/aclureno.html)

- The Internet is the large system of many connected computers around the world, which people use to communicate with each other.

- The Internet is a worldwide linkage of computers joined by telephone lines and fiber optic cables. The term "Inter" refers to the fact that it is an international connection, and the "net" is short for network (a connection of two or more computers that share their resources).

Let us also consider following other definitions of Internet:

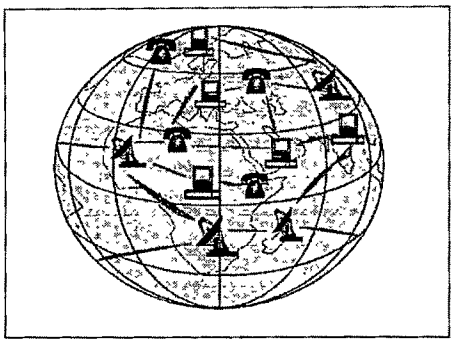
The Internet is a super-network. It connects many smaller networks together and allows all the computers to exchange information with each other. To accomplish this all the computers on the Internet have to use a common set of rules for communication. Those rules are called protocols, and the Internet uses a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). Many people equate the World Wide Web with the Internet. In fact, the Internet is like the highway, and the World Wide Web is like a truck that uses that highway to get from place to place. (See- www.wings.avkids.com/SPIT/glossary.html)

The interconnected network of networks that are sometimes referred to as the Information Superhighway. The Internet is a loosely organized series of computer networks where no one network or computer is essential to the operation of the whole. (See- www.cyberdog.org/defs.html)

Further Benzine and Gerland gives us the following definition [8]
(a) Generally (not capitalized), any collection of distinct networks working together as one.
(b) Specifically (capitalized), the world wide "network of networks" that are connecting each other into one single logical network all sharing a common addressing scheme (using the IP protocol and other similar protocols). The Internet provides file transfer, remote login, electronic mail, and other services.

From this definition we can infer that the Internet is nothing more than thousands of networks that are connected to each other (usually by way of telephone lines) in such a way that they can understand each other. The mechanism that enables the computers of the world to understand each other is a set of uniform rules that lays down the basic foundation of understanding between different computers. This is known as the Internet Protocol.

Concept map of Internet



The figure shows that computers all over the world are connected via telephone lines and broadband cables. It's a big matrix/cobweb of Internet connected computers. Messages are transformed through these cable/telephone lines. There is no centralized control over the way messages passes. Thus it is a global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions. (See-www.webopedia.com)

Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a *host*, is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well. Many people use the terms *Internet* and *World Wide Web* interchangeably, but in fact the two terms are not synonymous. The Internet and the Web are two separate but related things. The *Internet* is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Information that travels over the Internet does so via a variety of languages known as protocols.

The *World Wide Web*, or simply *Web*, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet.

4. ORIGIN AND GROWTH OF INTERNET

The birth and history of the Internet is very interesting. Some thirty years ago, the RAND Corporation, America's foremost Cold War think-tank, faced a strange strategic problem. How could the US authorities successfully communicate after a nuclear war? (9)

Post nuclear America wanted a command-and-control network, linked from city to city, state-to-state, and base-to-base, which can withstand the nuclear attack. But, no matter how thoroughly that network was protected; its switches and wiring were always being vulnerable to the impact of atomic bombs. A nuclear attack would reduce any conceivable network to tatters. Another question was, how would the network itself be commanded and controlled? Any central authority would be an obvious and immediate target for an enemy missile. The center of the network would be the very first place to go. RAND mulled over this grim puzzle in deep military secrecy, and arrived at a daring solution. The RAND proposal (the brainchild of RAND staffer Paul Baran) was made public in 1964. In the first place, the network would have no central authority. Furthermore, it would be designed from the beginning to operate while in tatters. The principles were simple. The network itself would be assumed to be unreliable at all times. It would be designed from the get-go to transcend its own unreliability. All the nodes in the network would be equal in status to all other nodes, each node with its own authority to originate, pass, and receive messages. The messages themselves would be divided into packets, each packet separately addressed. Each packet would begin at some specified source node, and end at some other specified destination node. Each packet would wind its way through the network on an individual basis.

During the 60s, this intriguing concept of a decentralized, blast proof, packet-switching network was kicked around. The National Physical Laboratory in Great Britain set up the first test network on these principles in 1968. Shortly afterward, the Pentagon's Advanced Research Projects Agency decided to fund a larger, more ambitious project in the USA. The nodes of the network were to

be high-speed supercomputers (or what passed for supercomputers at the time). These were rare and valuable machines, which were in real need of good solid networking, for the sake of national research-and-development projects. In mid of 1969, the first such node was installed. By December 1969, there were four nodes on the infant network, which was named ARPANET (ARPANET: Washington spent millions on the system. In 1969 the US Government-backed Advanced Research Projects Agency (ARPA) and the National Physical Lab in Britain developed the precursor of today's Internet. The original network, ARPANET, had four users. It was turned over to the US Defense Communications Agency in 1975) after its Pentagon sponsor. The four computers could transfer data on dedicated high-speed transmission lines. They could even be programmed remotely from the other nodes. Thanks to ARPANET, scientists and researchers could share one another's computer facilities by long-distance. This was a very handy service, for computer-time was precious in the early '70s. In 1971 there were fifteen nodes in ARPANET; by 1972, thirty-seven nodes. And it was good.

By the second year of operation, however, an odd fact became clear. ARPANET's users had warped the computer-sharing network into a dedicated, high-speed, federally subsidized electronic post- office. The main traffic on ARPANET was not long-distance computing. Instead, it was news and personal messages. Researchers were using ARPANET to collaborate on projects, to trade notes on work, and eventually, to downright gossip and schmooze. People had their own personal user accounts on the ARPANET computers, and their own personal addresses for electronic mail. Not only were they using ARPANET for person-to-person communication, but also, they were very enthusiastic about this particular service -- far more enthusiastic than they were about long-distance computation. It wasn't long before the invention of the mailing list, an ARPANET broadcasting technique in which an identical message could be sent automatically to large numbers of network subscribers. Interestingly, one of the first really big mailing lists was "SF- LOVERS," for science fiction fans. Discussing science fiction on the network was not work-related and was frowned upon by many ARPANET computer administrators, but this didn't stop it from happening. Throughout the '70s, ARPA's network grew. Its decentralized

structure made expansion easy. Unlike standard corporate computer networks, the ARPA network could accommodate many different kind of machines. As long as individual machines could speak the packet-switching language of the new, anarchic network, their brand names, and their content, and even their ownership, were irrelevant. The ARPA's original standard for communication was known as NCP, "Network Control Protocol," but as time passed and the technique advanced, NCP was superceded by a higher-level, more sophisticated standard known as TCP/IP. TCP, or "Transmission Control Protocol," converts messages into streams of packets at the source, and then reassembles them back into messages at the destination. IP, or "Internet Protocol," handles the addressing, seeing to it those packets are routed across multiple nodes and even across multiple networks with multiple standards.

As early as 1977, TCP/IP was being used by other networks to link to ARPANET. ARPANET itself remained fairly tightly controlled, at least until 1983, when its military segment broke off and became MILNET. But TCP/IP linked them all. And ARPANET itself, though it was growing, became a smaller and smaller neighborhood amid the vastly growing galaxy of other linked machines. As the '70s and '80s advanced, many very different social groups found themselves in possession of powerful computers. It was fairly easy to link these computers to the growing network-of- networks. As the use of TCP/IP became more common, entire other networks fell into the digital embrace of the Internet, and messily adhered. Since the software called TCP/IP was public-domain, and the basic technology was decentralized and rather anarchic by its very nature, it was difficult to stop people from barging in and linking up somewhere-or-other. In point of fact, nobody wanted to stop them from joining this branching complex of networks, which came to be known as the "Internet." Connecting to the Internet cost the taxpayer little or nothing, since each node was independent, and had to handle its own financing and its own technical requirements. The more, the merrier. Like the phone network, the computer network became steadily more valuable as it embraced larger and larger territories of people and resources. A fax machine is only valuable if everybody else has a fax machine. Until they do, a fax machine is just a curiosity. ARPANET, too, was a curiosity for a while. Then computer-networking became an utter necessity.

In 1984 the National Science Foundation got into the act, through its Office of Advanced Scientific Computing. The new NSFNET [10] set a blistering pace for technical advancement, linking newer, faster, supercomputers, through faster links, upgraded and expanded, again and again, in 1986, 1988, and 1990. And other government agencies leapt in: NASA, the National Institutes of Health, the Department of Energy, each of them maintaining a digital satrapy in the Internet confederation. The nodes in this growing network-of-networks were divided up into basic varieties. Foreign computers, and a few American ones, chose to be denoted by their geographical locations. The others were grouped by the six basic Internet "domains": gov, mil, edu, com, org and net. (Graceless abbreviations such as this are a standard feature of the TCP/IP protocols.) Gov, Mil, and Edu denoted governmental, military and educational institutions, which were, of course, the pioneers, since ARPANET had begun as a high-tech research exercise in national security. Com, however, stood for "commercial" institutions, which were soon bursting into the network, surrounded by nonprofit "orgs." (The "net" computers served as gateways between networks).

ARPANET itself formally expired in 1989, a happy victim of its own overwhelming success. Its users scarcely noticed, for ARPANET's functions not only continued but also steadily improved. The use of TCP/IP standards for computer networking is now global. In 1971, a mere twenty-one years ago, there were only four nodes in the ARPANET network. Today there are tens of thousands of nodes in the Internet, scattered over forty-two countries, with more coming on-line every day. Three million, possibly four million people use this gigantic mother-of-all-computer-networks.

The Internet is the most popular means of communication, and is the most important scientific instrument of the late twentieth century. The powerful, sophisticated access that it provides to specialized data and personal communication has increased the scientific research enormously. It is spreading faster than cellular phones, faster than fax machines. The number of "host" machines with direct connection to TCP/IP has been doubling every year since 1988. The Internet is moving out of its original base in military and research

institutions, into elementary and high schools, as well as into public libraries and the commercial sector.

Growth Chart of Internet

To give a sense of the Net's growth during the 1980s and '90s, according to Hobbes' Internet Timeline the number of Internet hosts (essentially the number of computers that connect to the Internet) has grown from 1,000 in 1984 to a million in 1992 to more than 16 million in 1997. **(PRINTED WITH PERMISSION)(source: Hobbes Internet Timeline – www.zakon.org/robert/internet/timeline)**

Growth

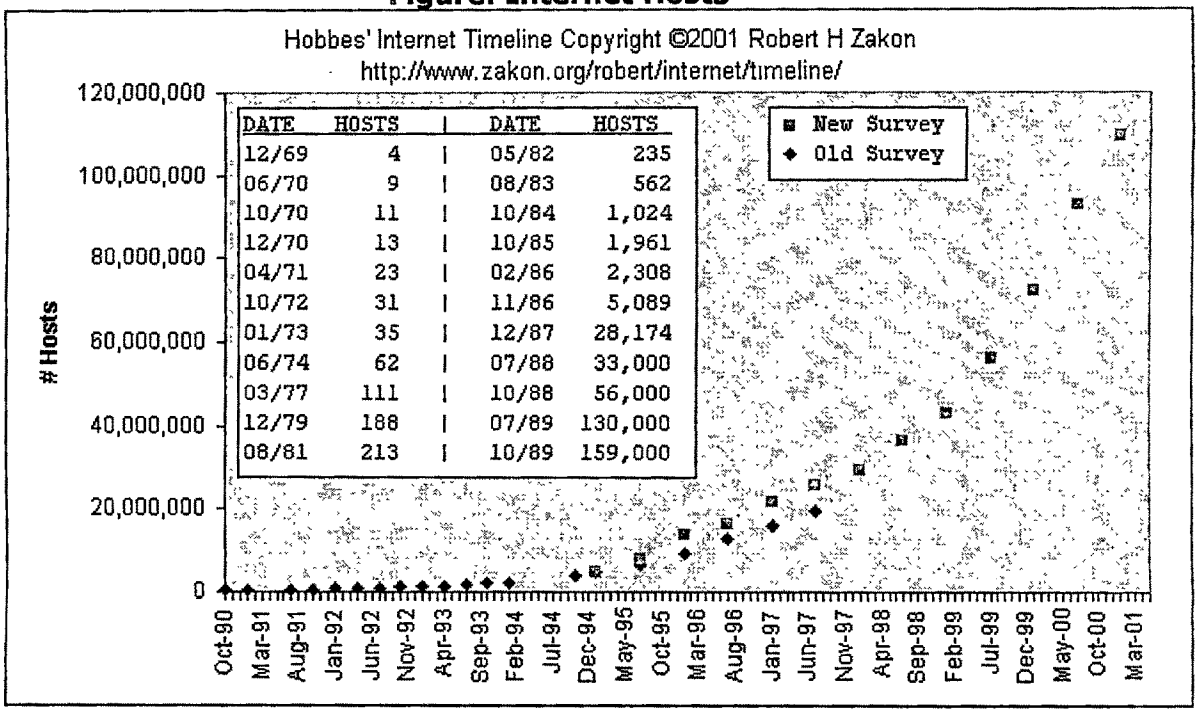
Internet | Networks | WWW | USENET | Security

Internet growth:

Date	Hosts	Date	Hosts	Networks	Domains
12/69	4	07/89	130,000	650	3,900
06/70	9	10/89	159,000	837	
10/70	11	10/90	313,000	2,063	9,300
12/70	13	01/91	376,000	2,338	
04/71	23	07/91	535,000	3,086	16,000
10/72	31	10/91	617,000	3,556	18,000
01/73	35	01/92	727,000	4,526	
06/74	62	04/92	890,000	5,291	20,000
03/77	111	07/92	992,000	6,569	16,300
12/79	188	10/92	1,136,000	7,505	18,100
08/81	213	01/93	1,313,000	8,258	21,000
05/82	235	04/93	1,486,000	9,722	22,000
08/83	562	07/93	1,776,000	13,767	26,000
10/84	1,024	10/93	2,056,000	16,533	28,000
10/85	1,961	01/94	2,217,000	20,539	30,000
02/86	2,308	07/94	3,212,000	25,210	46,000
11/86	5,089	10/94	3,864,000	37,022	56,000
12/87	28,174	01/95	4,852,000	39,410	71,000
07/88	33,000	07/95	6,642,000	61,538	120,000
10/88	56,000	01/96	9,472,000	93,671	240,000
01/89	80,000	07/96	12,881,000	134,365	488,000

The table shows how rapid there is a growth of Internet. In December 69 there were just four Hosts, which increased upto 19,540,000 by 1997. We can even see the remarkable growth of Networks from 650 in the year 1969 to Domain Names from 1,301,000.

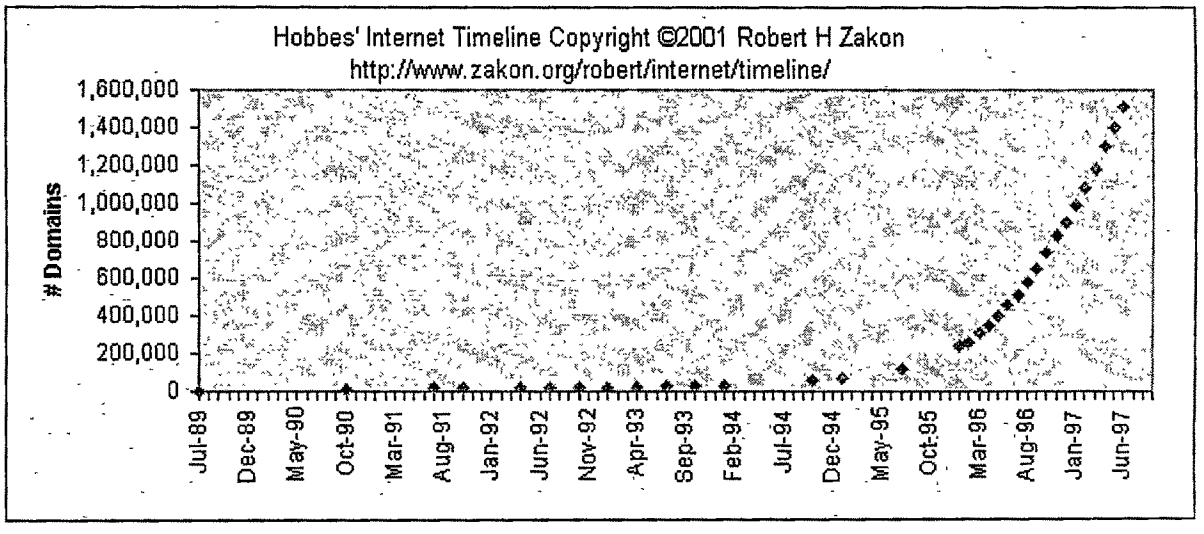
Figure: Internet Hosts



DATE	HOSTS	DATE	HOSTS
12/69	4	05/82	235
06/70	9	08/83	562
10/70	11	10/84	1,024
12/70	13	10/85	1,961
04/71	23	02/86	2,308
10/72	31	11/86	5,089
01/73	35	12/87	28,174
06/74	62	07/88	33,000
03/77	111	10/88	56,000
12/79	188	07/89	130,000
08/81	213	10/89	159,000

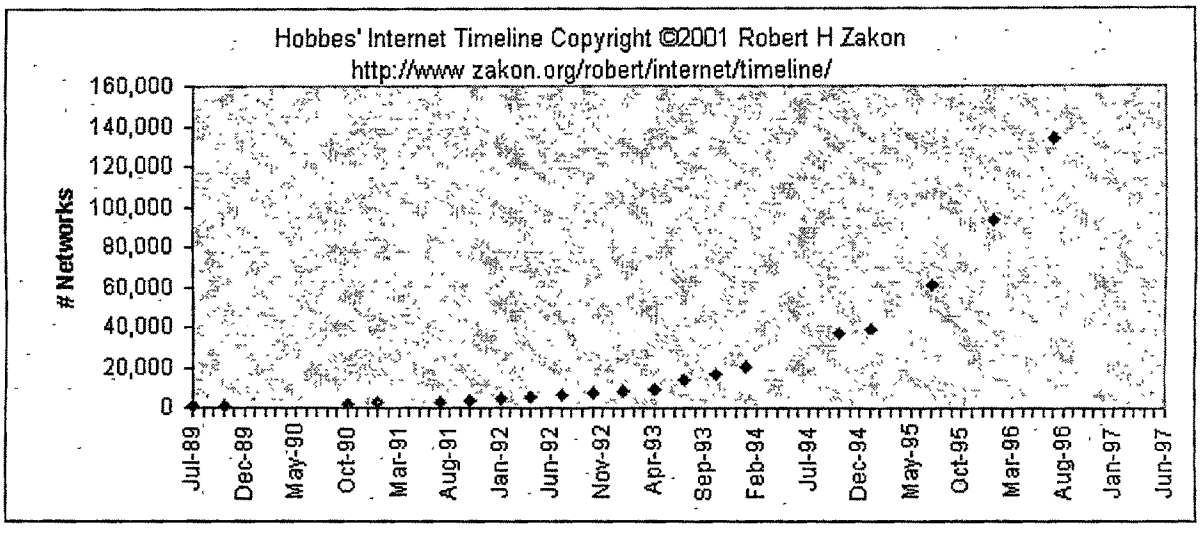
The above figures show us how fast there is a growth of Internet Hosts. By the end of March 2001 we can see that it has raised upto 120,000,000 Internet Hosts

Figure: Internet Domains



With the help of above-mentioned figure we can see that there is tremendous growth of Internet Domains from July 89 where by it was just 0, to January 97 were we can see that t has raised upto 1,600,000

Figure: Internet Networks



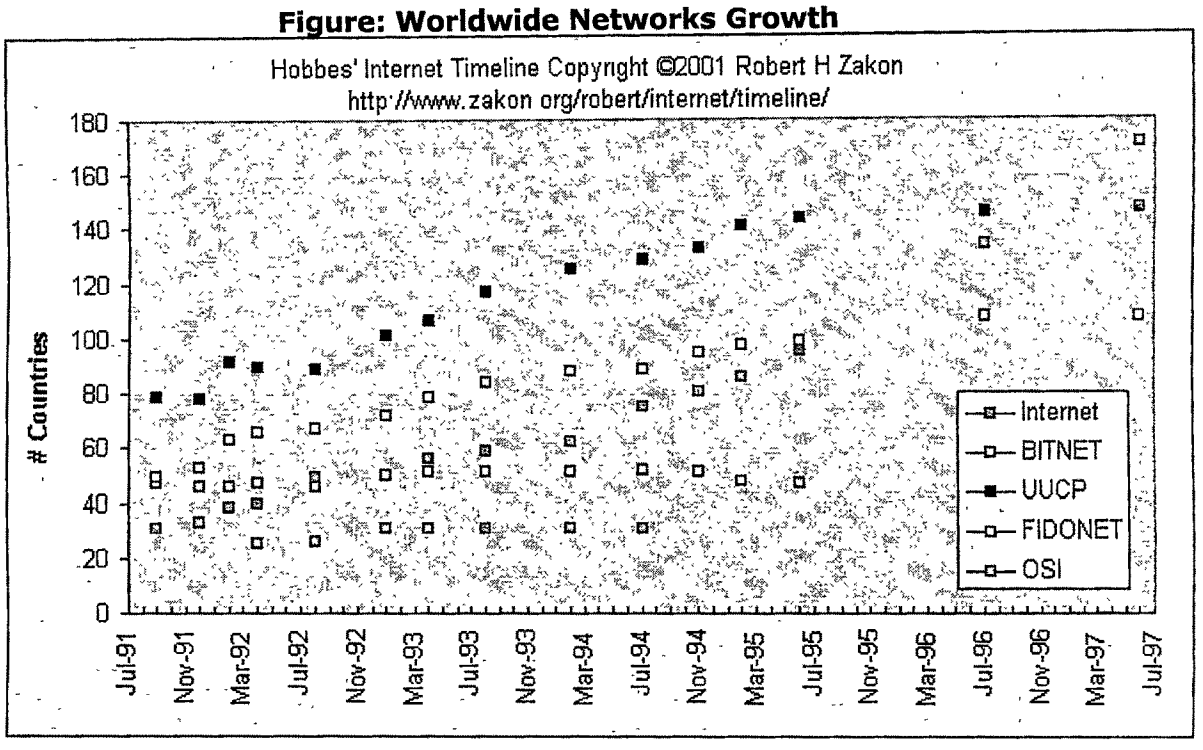
Even networks have increased from 20,000 in Dec.89 to 160,000 in January 1997. This is a remarkable achievement in its own way.

Worldwide Networks Growth: (I)nternet (B)ITNET (U)UCP (F)IDONET (O)SI

	# Countries				
Date	I	B	U	F	O
09/91	31	47	79	49	
12/91	33	46	78	53	
02/92	38	46	92	63	
04/92	40	47	90	66	25
08/92	49	46	89	67	26
01/93	50	50	101	72	31
04/93	56	51	107	79	31
08/93	59	51	117	84	31

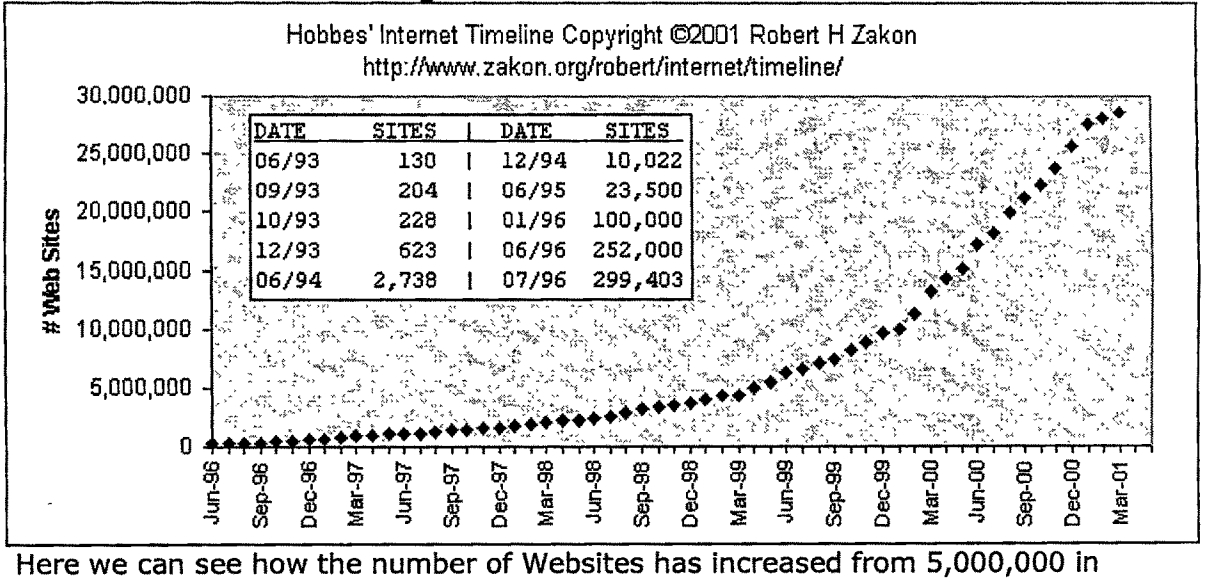
	# Countries				
Date	I	B	U	F	O
02/94	62	51	125	88	31
07/94	75	52	129	89	31
11/94	81	51	133	95	--
02/95	86	48	141	98	--
06/95	96	47	144	99	--
06/96	134	--	146	108	--
07/97	171	--	147	108	--

Figure: Worldwide Networks Growth



Sites = # of web servers (one host may have multiple sites by using different domains or port numbers)

Figure: WWW Growth



DATE	SITES	DATE	SITES
06/93	130	12/94	10,022
09/93	204	06/95	23,500
10/93	228	01/96	100,000
12/93	623	06/96	252,000
06/94	2,738	07/96	299,403

Here we can see how the number of Websites has increased from 5,000,000 in the year Sept. 1996 to 30,000,000 in the year March 01.

Why do people want to be "on the Internet?" One of the main reasons is simple freedom. The Internet is a rare example of a true, modern, functional anarchy. The Internet is also a bargain. The Internet as a whole, unlike the phone system, doesn't charge for long-distance service. And unlike most commercial computer networks, it doesn't charge for access time, either. In fact the "Internet" itself, which doesn't even officially exist as an entity, never "charges" for anything. Each group of people accessing the Internet is responsible for their own machine and their own section of line.

The Internet's "anarchy" may seem strange or even unnatural, but it makes a certain deep and basic sense. It's rather like the "anarchy" of the English language. Nobody rents English, and nobody owns English. As an English-speaking person, it's up to you to learn how to speak English properly and make whatever uses you please of it. Otherwise, everybody just sort of pitches in, and somehow the thing evolves on its own, and somehow turns out workable. And interesting. Fascinating, even. Though a lot of people earn their living from using and exploiting and teaching English, "English" as an institution is public property, a public good. Much the same goes for the Internet. Would English be improved if the "The English Language, Inc." had a board of directors and a chief executive officer, or a President and a Congress? There'd probably be a lot fewer new words in English, and a lot fewer new ideas. People on the Internet feel much the same way about their own institution. It's an institution that resists institutionalization. The Internet belongs to everyone and no one. Still, its various interest groups all have a claim. Business people want the Internet put on a sounder financial footing. Government people want the Internet more fully regulated. Academics want it dedicated exclusively to scholarly research. Military people want it spy-proof and secure. And so on and so on.

All these sources of conflict remain in a stumbling balance today, and the Internet, so far, remains in a thrivingly anarchical condition. Once upon a time, the NSFnet's high-speed, high-capacity lines were known as the "Internet Backbone," and their owners could rather lord it over the rest of the Internet; but today there are "backbones" in Canada, Japan, and Europe, and even

privately owned commercial Internet backbones specially created for carrying business traffic. Today, even privately owned desktop computers could become Internet nodes. You can carry one under your arm. Soon, perhaps, on your wrist.

5. HOW INTERNET WORKS

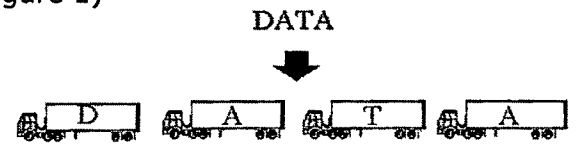
At the most basic level, the Internet connects two computers to each other and allows them to communicate back and forth. By the late 1990's the Internet became the most important part of our lives.

This connection follows varying routes. A computer user does not know where the computer to which they are connecting physically exists. When the Internet was created in the 1960's and 1970's, it was designed to maximize the connection speeds between computers by the use of "line testing" and "automatic routing" to the fastest route so that if one link goes down, traffic is just routed around it. The system determines the fastest route between locations, and then uses it.

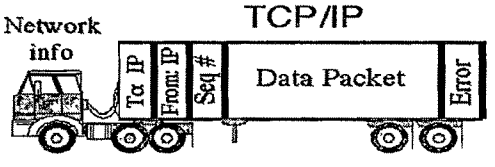
To understand how Internet works let us take one example. At the outset it is worth mentioning that computer breaks up the information into little parts called as "packets". These packets are about the size of three lines of e-mail. The post office is a good analogy to the Internet. Imagine a manuscript that must be sent from Los Angeles to New Delhi. Now assume that for some reason it must be broken onto 15 different parts, labeled part 1 of 15, part 2 of 15, and so on. These 15 different packages or packets are loaded into different trucks, which take different routes to New Delhi. When they arrive in New Delhi, these packets are reassembled into the manuscript. This is basically the way that the Internet works, but much faster because it takes just seconds for all 15 packets to be received across the country. Sometimes all 15 packets take the same route, and other times they can take up to 15 different routes.

Now let us see how packet switching system works. Packet switching works like this. In order to transfer the information over a network, it is first broken into

"packets". The figure shows that the information "DATA" is broken into single letters D + A + T + A. This each packet (letter) will travel by different route to reach the destination, which may be in the same country or in different country altogether. (Figure 1)



TCP/IP breaks the data into small packets (packages) for transporting over the Internet. Each packet contains information about the sender, destination, and quality control data with error correction. The packets are sent (routed) along the fastest pathway available to the network at the time. The packets sometimes follow different routes to the destination because of traffic on the network. (Figure 2)



TCP/IP is able to break the data into chunks of 64 bytes. This may not mean much now but a single letter or a number from 0 to 9 is equal to one byte. A byte is broken down into 8 smaller parts called bits. Bits are represented by either a 1 or 0 that the computer interprets as the state of on or off. The computer manipulates the 1s and 0s by using the rules of binary math.

Example:

bits vs. Bytes , Bye = 3 characters, 1 character = 1 Byte, Bye = 3 Bytes, 8 bits = 1 Byte

Bye = 24 bits, 1 bit = 0 or 1, Bye = a combination of 24 0s and 1s

One great appeal of this system to the US Govt. was that if a nuclear bomb ever knocked out parts of the military network, data would be "smart" enough to find its way across other parts of the network that remained intact. The particular route that the packet took would be unimportant. Only final results would count.

Basically, the packet would be tossed like a hot potato from node to node to node, more or less in the direction of its destination, until it ended up in the proper place. If big pieces of the network had been blown away, that simply

wouldn't matter; the packets would still stay airborne, lateralled wildly across the field by whatever nodes happened to survive. This rather haphazard delivery system might be "inefficient" in the usual sense (especially compared to, say, the telephone system) -- but it would be extremely rugged. (How Internet Works - see – www.seamonkey.ed.asu.edu/~storslee/net/gasu.html)

6. INTERNET IS A GLOBAL COBWEB

In 1996, the on-line community was 37 millions, which rose to 63 million in 1998 and it will cross 200 million by 2004. The Organization for Economic Co-operation and Development estimates global e-commerce sales of US $ 6500 billion in 2002. Thus Internet is a big matrix/cobweb. A hacker attempting to attack the computers at International Business Machines (IBM) does not know, if those computers are in the same state as the criminal or in a different state. Even if the computers are in the same state, the criminal doesn't know whether the route to IBM's computers will travel between multiple states or stay in the same state. Because of the decentralised design of the Internet, the Internet it self determines the route by which the user's activity moves. The user may be in one state, the accessed computer is in an adjacent state, but because of other traffic along the networks, the fastest route between the two points may cross many, many more states.

The headless, anarchic, million-limbed Internet is spreading like bread mold. Any computer of sufficient power is a potential spore for the Internet, and today such computers sell for less than $2,000 and are in the hands of people all over the world. ARPA's network, designed to assure control of a ravaged society after a nuclear holocaust, has been superceded by its mutant child the Internet, which is thoroughly out of control, and spreading exponentially through the post-Cold War electronic global village. The spread of the Internet in the 90s resembles the spread of personal computing in the 1970s, though it is even faster and perhaps more important. More important, perhaps, because it may give those personal computers a means of cheap, easy storage and access that is truly planetary in scale. The future of the Internet bids fair to be bigger and

exponentially faster. Commercialization of the Internet is a very hot topic today, with every manner of wild new commercial information- service promised. Or so it's hoped -- and planned, the real Internet of the future may bear very little resemblance to today's plans. Planning has never seemed to have much to do with the seething, fungal development of the Internet. After all, today's Internet bears little resemblance to those original grim plans for RAND's post- holocaust command grid. It's a fine and happy irony.

7. WHO RUNS THE NET?

First-time Internet users are often surprised by how hard it can be just to set up a computer with Internet access. Why isn't it as simple as hooking up cable TV or a telephone? Once online, new users are also surprised - and often frustrated - by the lack of organization or clear authority. "Isn't anyone in charge here?" they wonder. "Who runs the Net?" The truth is that no one runs the Internet. At least not the way that government rigidly control telephone, TV, and postal service in India. The roots of this decentralization lie in the Internet's beginnings as Arpanet, a "network of networks" funded by the US Department of Defense in the late 1960s. Created to connect disparate networks at campuses and laboratories around the US, Arpanet was designed so that if one site's computers or network went down, network traffic could take an alternate path to its final goal, rather than having to wait for repairs at that site. Without this architecture, the Internet would be far more prone to outages and slow-downs than it is now. Nonetheless, the Internet requires large-scale cooperation on many complicated technical and organizational matters in order to function. Several important bodies make the Internet work by setting recognized guidelines for hardware, software, and networks to communicate with one another. Your email address is a good example of the combination of organization and independence that makes the Internet work. Let's say your username is jonathan@wired.com. The part after the @ sign is the domain name, which specifies what local portion of the Internet your mail should be sent to. Domain names have to be unique - there can't be one wired.com in San Francisco and another wired.com in Bangalore - so there needs to be a

recognized governing body for Internet domain names. Domain names are handled in the United States by the InterNIC, or Internet Network Information Center. A cooperative activity between the National Science Foundation, AT&T, and Network Solutions Inc., InterNIC has a federal contract to provide a centralized directory of Internet domain names. For example, "wired.com" is registered with InterNIC so that only one company can use it. Within a given domain, the local Internet Service Provider controls matters like how email is routed and what username (the part ahead of the @ sign) you can have. For example, whether you get to pick your own email name or are forced to use one chosen for you is up to your company, school, or service provider.

The Internet works, not because of strong-armed authority, but because of cooperation and conformance to technical standards. Standards have an almost sacred aura on the Net, because they are the only way to ensure that different people using different hardware and software can communicate. People and companies that deviate from accepted standards face angry complaints, boycotts, and even lawsuits from other Net users. Several globally accepted standards bodies solicit proposals for Net use that are then formally reviewed by experts. Not surprisingly, many new standards are based on pre-existing patterns of use.

The Internet Engineering Task Force (IETF) is an international working group that sets standards for the software protocols that let computers and computer programs talk to one another on the Net. Amazingly, the Task Force is not a formal group of people, but remains open to any interested member. As the group's Web site states, "There is no membership in the IETF. Anyone may register for and attend any meeting. The closest thing there is to being an IETF member is being on the IETF or working group mailing lists." In other words, all you have to do to become an Internet standards contributor is participate! The Task Force takes existing, informal protocols and creates standardized versions of them through its "Request for Comments" documents, or RFCs. Among many other things, these documents describe how email servers talk to one another, how multimedia can be encoded in email, and how Web browsers and servers talk to one another.

The hardest thing to control on the Internet is the content that's being distributed - it's the best (and sometimes worst) thing about the Net. What began, as a project to serve US researchers has become a worldwide network of instantaneous access to information for millions of people around the globe. The same decentralized design that makes it impossible to shut down all of the Internet's hardware and software makes it impossible to stop people from transmitting whatever words, pictures, and software they please.

Of course, this free flow of information also creates new problems. Parents have difficulty blocking out information they deem unsuitable for their children. Copyright laws are almost impossible to enforce. Governments can't easily regulate information on the Net. Local boundaries and laws are almost impossible to apply to the Net - without unplugging it altogether. Net pundits often joke that (in Stewart Brand's words) "information wants to be free." To put it another way: No matter how hard you try to control information, it will find a way to free itself in order to be disseminated as widely as possible. Some control is possible: Secure systems for credit card transactions and private conversations seem to work well enough that people trust and use them, and filtering software offers a certain amount of control over unwanted Web content and email. But if you're looking for a higher authority to help you out, you're largely out of luck; few authorities can act as Net police, and none of them can act internationally. In the end, the answer to "Who runs the Net?" is both everyone and no one.

(Net Nuts & Bolts – see: www.hotwired.lycos.com/webmonkey/guides/net/runs.html)

8. FUTUER OF INTERNET

The Internet is currently expanding faster than television, radio and the printing press did. At a growth rate of approximately two million new users each month, it is sure to continue to transform virtually every area of our lives. Continuing developments in Internet access, speed and security will likely produce these changes in the foreseeable future: an explosion of commerce on the Internet.

Once major credit companies consider the Internet completely safe and secure, purchasing objects from virtual stores will become commonplace for all of us. an increasing amount of information will make the transition from printed media to a primarily digital existence. Some predict that the Baby Boomer generation is the last generation that will buy a daily printed newspaper...

Footnotes

1. See - www.isc.org - Statistical reports
2. Towards Digital equality – See: www.isc.org.
3. Matrix Information Services Inc. - See: www.mids.org.
4. Computer Industry Almanc – www.c-I-c.com/1`99911iu.htm
5. Europe and Asia play Catch-up with US E-marketer – See -www.e-land.com/estas/011100_
6. See- www.e-lamd.com/estas/011100_
7. Internet Protocol. The Internet Protocol is the network layer for a connectionless, best-effort packet switching protocol.
8. See: www.geocities.com/Athens/academics/5090/chapter2.html
9. See: Cyberspace - www.aces.uiuc.edu/AIM/scale/index.html
10. NSFnet: A network catering to academic institutions and military researchers was launched by the US National Science Foundation in 1987 Regional networks were connected to the NSF 'backbone' and to a similar network developed by the NASA space center in Houston