CHAPTER TWO

NATURE, FORMS AND REGULATION OF CYBER SPACE AND CYBER CRIMES
CHAPTER TWO
NATURE, FORMS AND REGULATION OF CYBERSPACE AND CYBER CRIME

I. INTRODUCTION
Cyber crimes is a generic term that covers the entire range of crimes that involve computers or computer networks either as its target, or as an instrumentality or associate. Any criminal activity that takes place in the so-called cyberspace comes under the purview of the term. As in the real world in the cyber world too, the criminal conduct is not limited to any specific type. The criminal conduct in cyber world covers the entire cyber activities, beginning from stealing of computer hardware to stealing of identities of the Net users.

The impact of cyber crime is also not limited to any particular target groups. As the entire human activities are increasingly being brought under the influence of Information Technology, there is no activity that stands immune from the impact of cybercrimes. When every activity depends on Information Technology as infrastructure, naturally all these activities become vulnerable to cybercrimes. Air Traffic control, Financial and banking transactions, Online trade, Stock exchange transactions, Personal data (particularly that of medical, financial and other information of confidential nature), Research and developments projects, scientific and technological processes. The list is unending. This is true to the demographic profile of potential victims too. Cybercrime is not limited to

those who are computer users or Internet users but may affect any and every person in this world. For example, when an hospital computer is hacked and prescription details are manipulated by a cracker, the patient who is going to receive the wrong medicine will bear the impact of this cybercrime though he may personally think that he has nothing to do with cyber world²

II. NATURE OF CYBER SPACE

The most important characteristic of the cyber world is the lack of distance and borders in it. Major advancements in technology are bringing people together worldwide. In the information superhighway called cyberspace, persons in the next room and persons in the farthest country are equal in terms of distance and the technology brings together those seeking to engage in illicit activity and thus assists in the construction of criminal enterprises. For even a relatively minor crime committed in one of the Indian villages through computer networks, the investigation might extend to the whole world.

Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location. Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial

delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another\textsuperscript{3}. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a virtual space consist of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction.

\textbf{A. SOPHISTICATION, SPEED AND ACCURACY}

Sophistication, Speed and Accuracy are some of the characteristics that make Internet. No wonder criminals also are attracted to the cyber world by these attributes. They have found ways to employ information technology to commit traditional forms of crime in more sophisticated and faster ways. An appropriate example of this is the piracy of intellectual property that is plaguing the entertainment industry worldwide. Through the use of powerful computers and the Internet, major criminal organizations are funding themselves through the global production, sale, and distribution of copyrighted materials, thus graduating this problem from isolated efforts to a level of organized crime. The ability of digital technologies to make accurate copies is creating headaches to law enforcement agencies worldwide, in the form of fake currencies that are hardly distinguishable from the originals.

\textsuperscript{3} David R. Johnson and David G. Post, Law and Borders- The rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996)
B. DIVERSITY AND PLURALITY IN VICTIMISATION

As already stated above cyber crimes does not discriminate while victimising people. An individual who gives his personal details in response to a query while submitting a form to his government, as a part of e-governance, might find the same being misused by international criminals in pursuing their crimes. Children who frequent chat rooms might fall prey to the paedophiles prowling such chat rooms searching for potential victims. A woman might find her being harassed by a maniac stalker through e-mails or even worse may find her name and address posted in a web site advertising sexual services. A bank may find itself the victim of a large-scale fraud committed by one of its employees having access to its computers in which he siphons crores of rupees by transferring small amounts from the accounts of its customers. A corporate body might find itself a victim of cyber extortion by a hacker who threatens to make some confidential information available to public or its competitors, unless it pays a huge sum to the hacker. In short the list of potential victims of cybercrimes is endless.

United State Government's report, 'The National Strategy to Secure Cyberspace', in the context of the need to ensure cyber security, stated the extend of diversity and plurality of victimisation in cybercrimes, in the following words:

"Cyberspace security requires action on multiple levels and by a diverse group of actors because literally hundreds of millions of devices are interconnected by a network of networks. The problem of cyberspace security can be best addressed at Home to Global Level.

C. HOME TO GLOBAL VULNERABILITIES

Though not a part of a critical infrastructure the computers of home users can become part of networks of remotely controlled machines that are then used to attack critical infrastructures. Undefended home and small business computers, particularly those using digital subscriber line (DSL) or cable connections, are vulnerable to attackers who can employ the use of those machines without the owner's knowledge. Groups of such "zombie" machines can then be used by third-party actors to launch denial-of-service (DoS) attacks on key Internet nodes and other important enterprises or critical infrastructures.

Large Enterprises

Large-scale enterprises (corporations, government agencies, and universities) are common targets for cyber attacks. Many such enterprises are part of critical infrastructures. Enterprises require clearly articulated, active information security policies and programs to audit compliance with cyber security best practices. According to the U.S. intelligence
community, American networks will be increasingly targeted by malicious actors both for the data and the power they possess.

Critical Sectors/Infrastructures

When organizations in sectors of the economy, government, or academia unite to address common cyber security problems, they can often reduce the burden on individual enterprises. Such collaboration often produces shared institutions and mechanisms, which, in turn, could have cyber vulnerabilities whose exploitation could directly affect the operations of member enterprises and the sector as a whole. Enterprises can also reduce cyber risks by participating in groups that develop best practices, evaluate technological offerings, certify products and services, and share information. Several sectors have formed Information Sharing and Analysis Centers (ISACs) to monitor for cyber attacks directed against their respective infrastructures. ISACs are also a vehicle for sharing information about attack trends, vulnerabilities, and best practices.

National Vulnerabilities

Some cyber security problems have national implications and cannot be solved by individual enterprises or infrastructure sectors alone. All sectors share the Internet. Accordingly, they are all at risk if its mechanisms (e.g., protocols and routers) are not secure. Weaknesses in widely used software and hardware products can also create problems at the national
level, requiring coordinated activities for the research and development of improved technologies. Additionally, the lack of trained and certified cyber security professionals also merits national-level concern.

Global

The worldwide web is a planetary information grid of systems. Internationally shared standards enable interoperability among the world's computer systems. This interconnectedness, however, also means that problems on one continent have the potential to effect computers on another. We therefore rely on international cooperation to share information related to cyber issues and, further, to prosecute cyber criminals. Without such cooperation, our collective ability to detect, deter, and minimize the effects of cyber-based attacks would be greatly diminished.

III. FORMS OF CYBER CRIMES

The Information Technology revolution is unparalleled before attempting to undertake any description of current forms of criminality that exist in the cyberspace, it is only prudent to make a disclaimer that the list is not limited to the one being discussed here. The list of cybercrimes is a never ending one; with each day newer forms of criminal behaviour are being

---

witnessed in the cyber world. Having said that, the type of cybercrimes prevalent today are briefly discussed below:

A. Crimes Affecting Individuals

(i) Infringement of Privacy

The most important aspect of computers is their ability to store, manipulate and transmit data much faster than any manual system of record keeping. In today's world increasing use of computer networks including Internet for storing and transmitting of personal data, under various circumstances makes it possible for collating all information about a person, which he himself may not even be aware of. Some information might have been given voluntarily, yet some might have been captured during some transaction that he has entered into or he was subjected to. For example, when a person undergoes a medical check up his medical data is fed into the hospital computer. Anyone with access, whether authorised or unauthorised can obtain this data and make use of it as he deems fit. With enough resources anyone individual or organisation could act as a 'big brother' and take advantage of any individual today, by virtue of all the information that he can collect about him.

The dangers of allowing the data to flow with absolute freedom across the network need no emphasis. Such flow can threaten even the existence and competitiveness of the organisations and also the security of the States. In the case of individuals lack of privacy can have serious repercussions.

"Clear infringements of privacy became known especially in the area of traditionally protected professional secrets, especially concerning official secrecy as well as the requirement of confidentiality for officials, doctors,
lawyers and banks. Such data constituted the object of the offence in a South-African case, in which the offender-presumably through theft of magnetic tapes- obtained medical data of persons which (sic) had undergone an AIDS test; the confidential data was passed on to the employers of the affected persons6.

Thus, availability of the data in the cyberspace, for anyone with the capability to access, has brought up the issue of criminal infringements of 'privacy. Right to privacy is considered as a fundamental right of the individuals in almost all the civilised world7. The dichotomy of protecting individual's right to privacy and the free flow of information across the networks and frontiers has, therefore, occupied the minds of nations across the globe. While it is easier to protect the individuals from defamation etc., within the traditional legal systems, the wholesome data protection requires more specialised and international efforts. The lack of certainty as to what amounts to an individual's right to privacy also compounds the problem further. Even the United Nations Declaration of Human Rights, at Article 12, states that every individual has a right to privacy, but does not define as to what the term privacy means. So, the objective of the legislative efforts has not been the controversial concept of right to privacy, but confined to 'providing a framework for finding a balance between the interests of the individual, the data user and the community at large'8.

6. Van der Merwe, in Sieber (Ed.) Information Technology Crime, 1994
7. Also see, Mark S. Merkow, & James Breithaupt, The E-Privacy Imperative, American Management Association (2002), New York
8 SD Warren and LD Brandeis, The Right to Privacy, Harvard Law Review,
Unfortunately, the Indian Information Technology Act, 2000, which was enacted to 'provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communications' does not give cyber-crimes the attention that it deserves. As a result, the Indian Act is silent on the need for protection of privacy in the cyber context. This Act however, contains an incidental provision under Section 72, which provides for penalty for breach of confidentiality and privacy in the limited context, where any person illegally and without the consent of the person concerned discloses any electronic record, book, register, correspondence, information, document or other material to which he got access under any of the provisions of the Act or any rules or regulations made thereunder.

Though many of the countries have adopted data protection laws, it is the Europe that has taken lead in this direction. As many as 25 European countries have some laws on this subject and some have even revised or amended their law. Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is a comprehensive effort to unify various legislative directions. This Convention was entered into since 'it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal

---

9. Preamble to the Information Technology Act, 2000
10. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, for complete Text see Appendices.
data undergoing automatic processing\textsuperscript{11}. It recognizes that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples, and requires the member States to ensure that appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorised access, alteration or dissemination. The Convention also requires that 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions also.

The Organisation for Economic Co-operation and Development had issued Guidelines\textsuperscript{12} in 1980, that called upon the countries to adopt good data protection practices in order to prevent unnecessary restrictions on trans border data flows. Similarly, United Nations has, adopt a set of guidelines for the regulation of computerized personal data files\textsuperscript{13}, with a section on 'Principles concerning the minimum guarantees that should be provided in national legislations' and another section on 'application of the guidelines to personal data files kept by the governmental international organisations'.

\begin{itemize}
\item \textsuperscript{11} Preamble of the Convention.
\item \textsuperscript{12} OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris.
\item \textsuperscript{13} Adopted by the UN General Assembly, vide Resolution No. 45/95 on 14 December 1990.
\end{itemize}
The infringement of privacy and the need for protection of data is not limited to individuals alone. It is more serious in case of commercial organisations and governments. For example, anyone who can get an access to the e-mail folder of a business organisation can effectively come to know the entire process by which it conducts its business. The danger lies in the fact that these electronic mails pass through the networks and anyone who has the control over it or has the access to it can keep a record of the data flow and sell it to the organisation's competitors. The responsibility of the service provider is also not clear where one's mail records get misused even when his staff obtain the information and misuses it for private gain, or personal embarrassment or even political or religious reasons.

(ii) Identity Theft

Identity theft undermines confidence in the integrity of commercial transactions and invades individual privacy. The term identity theft commonly refers to a host of frauds, thefts, forgeries, false statements and impersonations involving the use of another person's identifying information. It occurs when someone uses bits and pieces of information about an individual to represent himself as that victim for fraudulent purposes. Examples are obtaining credit cards and loans in someone else's name and then not paying the bills, renting an apartment, getting a cellular phone, purchasing a car or a home, etc. The most serious type of

identity theft is when the thief commits crimes in the victim's name and gives that person a criminal record. Identity theft facilitated by the Internet will grow as electronic commerce grow, which it is doing exponentially as internet provides to perpetrators low-cost, efficient methods for capturing the Identities of unsuspecting victims.

Since the transaction amounts to a fraud, the victim is not liable for the same. However, when the creditor calls him up to pay or the police knocks his door for some crime that he is not even aware of, the shock can be devastating and also he will have to run from pillar to post to prove his innocence. The identity theft occurs in the cyber scenario due to lack of data security. It could be either from the negligence of the victim himself in protecting his personal data or from the lack of data security in some computer where the data concerning the victim was stored.

Another form of identity theft, with more serious consequences, is the relatively latest form of cybercrime known as 'SMS Spoofing'. In this cybercrime the criminal(s), using a Web-based software steals another's identity in the form of his or her mobile phone number to send a message from a computer to some unsuspecting person. The message appears to the recipient as if he has received it from the victim. The potential danger of this crime has come to the light in an incident where a woman received a SMS from her husband's number that he was in deep trouble and he needed some large amount of cash. Since she received the SMS from her husband's cell number, she rushed out with the money. The movement
she stepped out of her house, she was attacked and the whole cash was stolen.\textsuperscript{15}

(iii) Cyber Stalking

Stalking is not a new form of crime. It has existed from time immemorial. However, it is only recently that it has received attention as a serious crime from the criminologists. Till then the activities that characterised stalking were dismissed as minor and not deserving any state intervention. Actions such as harassing phone calls, unsolicited gifts, persistent following and even domestic assaults were either not covered by legislation or simply could be dealt with other provisions under criminal law. But the term stalking acquired broad public recognition in the west during the mid-1990s when a number of criminal cases were widely reported in the media in which the offender had repeatedly subjected his or her victim to either criminal behaviour or forms of harassment which fell short of being criminal. Initially, stalking was considered as a phenomenon associated with celebrity, with obsessive fans following or trying to contact their idols. In response to the increasing number of incidents of stalking coming to the attention of the criminal justice system, new legislations were introduced in countries like UK and USA. The Protection From Harassment Act, 1997 of UK and Model Anti-stalking Code by the National Institute of Justice of USA, for the adoption by its States\textsuperscript{16}, are examples of these efforts.

\textsuperscript{15} Reported in SMS Spoofing: The new age cyber crime, The Times of India, Bangalore Edition dated 12 ju12004.
\textsuperscript{16} As many as 17 States in the US has adopted Anti-stalking legislations.
Model Anti-stalking Code issued by US National Institute of Justice defines the term stalking as "a course of conduct directed at a specific person that involves repeated visual or physical proximity, nonconsensual communication, or verbal, written or implied threats, or a combination thereof, that would cause a reasonable person fear." Some form of access to the victim is necessary to carryout any kind of stalking. With the computers and Internet bringing the world into our homes, access has become almost unlimited. Internet provides access to a vast amount of information, and provides forums for individuals from allover the world to meet one another in a relatively anonymous virtual environment. Though these contacts are mostly healthy and innocuous, it increases the possibility that anyone could become the target of unwanted attention.

Cyber stalking is only an extension of the physical form of stalking, the only difference being that in cyber stalking electronic mediums like Internet are used to pursue, harass or contact another in an unsolicited fashion. The term cyber stalking is used to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. The cyber stalking could be across the globe and anonymous and may not pause any physical threat at all. But it is an accepted fact that it is not just the physical aspect that distresses the victim but the unsolicited pursuit even in virtual world can become highly distressing. There are a

18. On cyber stalking also see, Wall, David, S., "Cybercrimes: New wine, no bottles."
wide variety of means by which individuals may seek out and harass individuals even though they may not share the same geographic borders, and this may present a range of physical, emotional, and psychological consequences that are sometimes devastating, to the victim. With the increasing number of people using Internet in their day-to-day life, the menace of cyber stalking is bound to grow in stature as a cyber crime.

B. Crimes Affecting Economy

One of the most important developments brought about by the Internet is the possibility of what is generally known as e-commerce. The way we conduct trade and business has been dramatically altered by the growth and development of new technologies and communications systems. This revolution is being led by the computers and the Internet, which are being used by businesses and the consumers on an increasingly large scale as a substitute for the traditional paper based transaction systems. The advantages are apparent, speed and cost effectiveness being the major plus points. E-commerce or the electronic commerce makes it possible to overcome the barriers of time and distance and allow people to carry on their trade across the national borders. However, these developments are not without any pitfalls. Since the cyber space has become where commerce and money is moving, it was not possible to keep the crime and criminals at bay. The criminals armed with technological sophistication has found it much easier to carry out their activities in the cyber world. During the 1970s fraudulent computer
manipulations were the starting point of the computer-related economic crime. However, today hacking has increasingly become a "basic offence" which is then used commit acts of espionage, software piracy, sabotage, as well as computer fraud\textsuperscript{19}. So let us start with the cybercrime of hacking.

(i) Hacking

The term 'computer hacking' traditionally describes the penetration of computer systems, which is not carried out with the aims of manipulation, sabotage or espionage, but for the pleasure of overcoming the technical security measures\textsuperscript{20}. However, with the increasing use of computer networks by commercial and military organisations, the potential of hacking as realized by criminals and it became the basis for almost all types of cybercrimes\textsuperscript{21}.

The hacking techniques depend upon the respective communication and security system that are used by a network or a computer. Traditional forms of hacking were based on the use of standard passwords, physically watching the user typing in the details or using confidence tricks by which the hacker persuades or deceives the user to reveal them. Though awareness about better password management has come about in the computer users, the advent of Internet has brought many new techniques


\textsuperscript{20} Supra

\textsuperscript{21} On hacking also See, D.P. Mittal, Law Of Information Technology (Cyber Law), (Delhi, Taxmann Allied Services Pvt. Ltd. Publishers (2000); Kaspersen
that are used in hacking and computer manipulations. Some of the major techniques that are used by hackers to get entry in to a computer system are as follows:

IP-Spoofing: This technique is used to gain unauthorized access to computers or networks from outside by pretending to be an authorised and trusted device inside the penetrated network. This is done through modification of IP addresses in data packet headers transmitted to an incoming port of the network's router.

Although the fake IP address is known as a valid address inside the network only, routers were not able to distinguish between data transmitted from outside or inside of network. Newer routers and firewalls offer protection against this kind of attacks.

DNS Spoofing: DNS spoofing describes the faking of hostmasks during the resolution of Internet hostnames. DNS or "Domain Name Service" provides the mapping between hostnames and IP addresses. Every access request on the Internet using the host's name has to be resolved to its IP address, which is done by communicating with a DNS-server which stores the hostmasks in databases. To perform the DNS spoofing attack, a hacker tries to intercept the communication and to send fake hostname mappings to the victim's computer. This can easily be done using malicious web applets downloaded by the attacked user himself. Once the applet is activated, the user's communication could be rerouted and the transmitted data could be gathered.
Web Spoofing: While IP and DNS spoofing depend on sophisticated technical knowledge, web-spoofing attacks use a much simpler approach. These are based on optical illusion in general. Hyperlinks on web pages can contain characters that make an address look real, but in fact lead to a wrong web site, e.g. replacing the letter "0" in the address <www.microsoft.com>. Most users would not suspect any malicious intention. In this example, the hacker would set up a web page asking for the input of sensible user information, e.g. credit card information.  

These methods evolved out of the use of new communication protocols like Internet Protocol (IP) or Hypertext Transfer Protocol (HTTP) used to run web servers. The hackers not only invent new ways to overcome security systems in the computers and networks but also make them public through Internet for other hackers to use. One hacker may make a new program to enter a particular network for just to beat the security system but the same techniques when known to a criminal will be used for illegal purposes. There are various kinds of hackers prowling the Internet and they have been categorized as follows:

Pioneers: those who are fascinated by evolving technology and explore it without knowing exactly what they are going to find., Scamps: hackers with a sense of fun who intend no overt harm.

Explorers: hackers motivated by a delight in breaking into computer systems. The more geographically distant, or more secure the target is, the greater the delight.

Game players: those who enjoy defeating software or system protection, with hacking seen as a sort of game itself.

Vandals: those who cause damage for no apparent gain.

Addicts: nerds who are literally addicted to hacking and computer technology21.

The Indian Information Technology Act, 2000 makes hacking an offence. The provisions contained in the Act is as follows:

66. Hacking with computer system.—(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

23. www.faculty.ncwc.edu/tocoimor/410/cuberspacelaw.htm, Cybercrime:
(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

70. Protected system.—(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer

The Internet as Crime Scene system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access a protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

It may be noticed that the Indian law limits the scope of hacking as an offence by making it applicable only where the hacker "destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means". Unauthorised entry is punished only when such entry is made into a 'protected system' as
defined in Section 70. However, distinguishing hackers on the basis of their intention or motivation does not serve any purpose most of the times. Even where the hacking was benign, the victim cannot differentiate it from vicious hackings and thus his confidence level on the system security is affected.

Unlike Indian Law, The Council of Europe Convention makes any unauthorized access an offence and calls upon member states to adopt legislations to establish the same as an offence, vide its Article 2, which states:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system".

(ii) Virus and other Malicious Programs

A malicious program is intended to cause harm to its victims. It includes Virus, Worm, Trojan Horses, Logic bombs and Hoaxes.
- A virus is a malicious program that infects an executable file and after infecting it causes that file to function some way other than what was its original function, and having the ability to propagate itself attaching to executable files like application programs, operating system, macros, scripts, boot sector of a hard disk or floppy disk etc. Running the executable file may make new copies of the virus. Virus by itself cannot make copies, but there are other programs that can copy itself and these programs are called 'worms'.

- Worms are malicious programs that usually does not alter or delete any files but only multiply itself and send those copies to other computers from the victim's computer. Releasing a worm into Internet causes slowing or clogging of network since the worms keep multiplying themselves at whichever computer they reach and then start sending copies to other computers. However, recently like "Klez" worm in 2002 have been introduced which have the properties of both virus and a worm, there by increasing the damage potential.

- A Trojan horse is an innocent looking program that contains functions unknown to its users. Hackers usually use these programs to collect data like passwords or credit card numbers. These programs could be either deposited by an outsider into the victim's computer or victim himself could download it from
some other computer thinking that it is some other useful program.

- A logic bomb is a malicious program that executes only when a particular event occurs. Once detonated the logic bomb makes the program to go into an infinite loop, crash the computer, delete data files, or some other damage to the computer or its data.

- A hoax is merely a false warning about existence of some malicious program.

Since the Internet functions on the basis of the interconnectivity of computer networks, it becomes possible for anyone to send viruses and other malicious programs to any computer, just like he sends an e-mail. Internet and e-mails are considered ideal for their spread. These programs created for a variety of reasons, can have many different effects, depending on the creator's intent. For example, some of the viruses are found to cause varied functions as follows:

"Clipper" scrambles all the data on a hard drive, rendering it useless.

"Gingrich" randomly converts word processing files into legalese often found in contracts. Victims can combat this virus by typing their names at the bottom of infected files, thereby signing them, as if signing a contract.
"Lecture" deliberately formats the hard drive, destroying all data, then scolds the user for not catching it.

"Melissa" infects a possibly confidential document on a victim's computer, then automatically sent that document and copy of the virus via e-mail to other people.

"SPA" examines programs on the hard disk to determine whether they are properly licensed. If the virus detects illegally copied software, it seizes the computer's modem, automatically dials 911, and asks for help.

"Osama Bin Laden" when opened shows the scene of Bin Laden committing suicide and the same time introduces a Trojan horse program in the recipient's system24.

Though some may be innocuous others can cause devastating effects by destroying the entire data contained in a computer system, thereby jeopardizing the activities of the individual or the organization in this era of computerisation and e-commerce. The ability of these programs to multiply and spread across the net make them more dangerous, apart from slowing down the network.

(iii) Computer Sabotage and Computer Extortion

With the increasing use of computer as a medium to store valuable data, and dependence of the governments, companies and individuals alike on computer networks and information technology in day-to-day affairs, computer sabotage is gaining importance. Earlier, sabotage was caused by physically destroying the computers by igniting or bombing a building. For insiders it is even easier to sabotage the system by using electrical short circuits or pouring saline solution over the hardware etc. In both these situations however, the likelihood of getting caught was high. But, with the advancement in the knowledge and technology more and more malicious programs are being used to sabotage the computer systems and carry out extortion. Prof. Dr. Ulrich Sieber cites the following incident as an example of computer sabotage\textsuperscript{25}: A German engineer erased the comments of a valuable computer program on the disc by using programs before leaving the company so that it could not be easily modified by other programmers due to which the company almost lost a contract worth DM 1 million.

Convergence of computer and other telecommunications systems leads to a situation where it is easier for anyone to tamper the communication systems like telephone exchanges and switching systems etc. The increasing dependency on the computer networks makes computer extortion another area of concern. Large amount of data, including that of

\textsuperscript{25} Prof. Dr. Ulrich Sieber, legal Aspects of computer related Crime in the Information Society, Prepared for the European Commission, 1998
confidential nature are kept in the computer hard discs and the criminals can obtain this information and then resort to extortion of the organisation or individual with threat to publish them. There were instances of banks being subjected to extortion by threat to publish their customer data, including that of customers who had presumably committed tax fraud offences. Prof. Sieber gives another example where computer extortion was carried out by an American scientist who distributed more than 20,000 floppy disks which supposedly contained information about the AIDS-virus, but instead encoded the user's hard disk when opening the stored files. By a corresponding announcement on the screen, the users were advised to transfer an amount of at least US $ 189 to a bank account in Panama in order to obtain the code for decoding the hard disc.

(iv) Computer Fraud

The term computer fraud denotes a sub-class of economic crimes that are being carried out by the help of computer networks and Internet in cyberspace. When the computer networks were Intranets, the computer frauds were limited to manipulations of data, by some insider, concerning invoices, account balance or payment of salary. With the Internet the computers are now interlinked globally and there by the possibilities of committing fraud from outside has increased.

The computer and Internet are being increasingly used to commit all sorts

26. On cyber frauds also see Piragoff, Donald K, "Computer Crimes and Other Crimes against Information Technology in Canada"
of fraud that are 'traditional' in nature. A study of the computer frauds reported in USA\(^{27}\), in 2001, shows that Internet auction fraud was by far the most reported offense, comprising 42.8% of referred complaints. Non-deliverable merchandise and payment account for 20.3% of complaints, and Nigerian Letter fraud made up 15.5% of complaints. Credit/debit Card fraud and Confidence fraud (such as home improvement scams and multi-level marketing) round out the top five categories of complaints referred to law enforcement during the year in USA.

Internet has certain inherent features that makes it ideal for fraudulent purposes: Cost-effectiveness, breadth of reach, difficulties in authenticating identity, anonymity, ease of personalizing appeals, and novelty\(^{28}\). A fraudulent Investment scheme may be advertised relatively cheaply on a credible looking website or by mass e-mailing, and reach millions of people across the world, making it much easier to locate those gullible enough to part with their cash.

One area where computer fraud is rampant is the on-line trading. In 1999, a survey was conducted at the University of Utah\(^{29}\) of Internet trading which was coordinated by Consumers International and funded by the European Union. Representatives of those groups bought more than 150 items from Web sites based in seventeen countries, and then tried to return

them. It was found that eight percent of the items ordered never arrived; many Web sites did not give clear information about delivery charges; a minority disclosed whether the laws of the seller's country or the buyer's country would apply in the event of a dispute, and only fifty-three percent had a return policy. In addition, only about thirteen percent of the sites promised not to sell customers' personal data to a third party and only thirty-two percent provided information on how to complain if there was a problem with a transaction. It is needless to say such affairs discredit the entire e-commerce and stems its growth.

Where goods and services are obtained on-line and paid for by using paper-based instruments, such as money orders or cheques, fraud may be perpetrated in the same ways as those which have operated in the past where these payment systems have been employed. The nature of Internet transaction makes it nearly impossible to find out in advance about individuals using accounts which have been opened through the use of false identification details, exceeding the credit balance held in cheque accounts, or counterfeiting or altering instruments themselves. Merchants may not be in a position to wait for cheques to be cleared prior to dispatching the goods or providing the services, thus leaving them open to fraud. Similarly, consumers may send off a cheque to a merchant they have no independent information about, who may be located in a foreign country, receive payment, and default on the agreement.
Another form of fraud perpetrated on Internet is related to so-called sex lines. In USA and Canada over 38,000 users could be convinced to download a picture viewer of several sex sites for free. The software enabled the user to view pornographic pictures over the Internet while seemingly not being charged for the service. However as soon as the user had started the program, it silently disconnected the users from their local Internet service provider, and reconnected them to the website rerouting the phone call to a telephone sex service in Moldova, first. As a result consumers were billed more than US$ 2 per minute by their long distance providers. After shutting down the picture viewer or web browser, the software kept the modem connected to Moldova, resulting in some long distance calls totaling several thousand US Dollars\textsuperscript{30}.

The Indian Information Technology Act, 2000 has carried out necessary amendments to the Indian Penal Code to bring computer frauds under the purview of traditional frauds. Similarly most of the countries have either passed new legislations or have carried out amendments in their criminal codes to make frauds committed on cyberspace Punishable.

(v) Computer Forgery and Counterfeiting

Closely related to computer fraud are the offences of computer forgery and counterfeiting. Guaranteeing the authenticity of any document is a basic necessity in any economy. One of the problems that were faced by

---

\textsuperscript{30} Prof. Dr. Ulrich Sieber, Legal Aspects of Computer Related Crime in the Information Society, Prepared for the European Commission, 1998
the international community while changing over to e-commerce was the question of authenticity of the electronic documents. Digital technology facilitates perfect reproduction of documents. By using a computer it is very easy to counterfeit a document like birth certificate, which can further be used in creating legitimate identification documents and then use the false identity to perpetuate any crime. Computers and the advanced printing technology keep the authorities on their toes with regard to counterfeiting of currency notes.

Section 74 of the Indian Information Technology Act, 2000 deals with fraud and forgery related to digital signature certificates only. The Section states; 'Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extend to one Lakh rupees, or with both'. So the Indian Act does not deal with forgery or fraud connected with other documents or situations. However, necessary provisions exist in the Indian Penal Code to deal with such offences and position is similar in most of the countries.

(vi) Theft of Telecommunication Services

As we have already seen the convergence of technologies make telecommunication systems highly dependent upon computer networks. The switching instruments and exchanges use the similar technology as in the routers of computer networks. It is therefore easy for a hacker to break
in a communication network's telephone switchboard and get access to dial-in/dial-out circuits and then make their own calls or provide these services to others. Frauds in Internet telephony causing huge losses to the telecommunication companies have been reported from all over the world.\(^{31}\)

Increasing use of mobile phone services offer another area for the criminals. It is easier for them to crack the code being used to connect the phone to the service provider and then use it for misusing the same. A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he should be the winning caller in several call-in contests held by local radio stations.\(^{32}\) The fruits of his scheme included two sports cars and $30,000 in cash. Internet-connected computers are subject to similar types of attacks. Routers—which are computers that direct data packets traveling on the Internet—are analogous to telephone switches and thus are tempting targets for skilled hackers who are interested in disrupting, or even rerouting, communications traffic on the network.

\(^{31}\) On cybercrimes against telecommunication services also see, Donn Parker and Susan H. Nycum "Computer Crime" Communications of the ACM, Volume 27 Number 4, April 1984

\(^{32}\) www.cybercrime.gov
(vii) Software Piracy and Other Copyright Violations

Copyright means the exclusive right of an author (or an owner as the case may be) to do or authorise others to do certain acts for the commercial exploitation of the copyrighted material, which may include literary, dramatic, musical and artistic works, cinematograph film and sound recordings. These rights are considered to be the quid-pro-quo that the society offer for the benefits accrued to it from the intellectual efforts of the creator of the work. Therefore, commercial exploitation of copyrighted materials by unauthorized persons amounts to a crime against society and is termed as piracy.

Among the economic crimes that are being committed in the cyberspace, one of the most critical is the copyright piracy. The importance of protecting the copyright of authors, be it that of a software program or a book, has received some form of recognition in the entire world. However, the nature and the extent of protection afforded by individual nations differ considerably, notwithstanding the efforts to standardize it through international treaties. Coupled with this is the problem of obscurity as to the very concepts what constitutes copyright violation. Nevertheless, protection of intellectual property rights is essential for the continued development of our knowledge and life. It is even more so in the case of computer software. Rapid turnover in the software technology make it imperative that the authors must be afforded with effective protection of rights to exploit their intellectual products.
A recent study undertaken by Business Software Alliance\textsuperscript{33} shows that as much as 36\% of the software installed on computers worldwide in 2003 was pirated, with emerging markets like India, China, and Russia remaining high piracy regions. Of the $80 Billion worth of software installed in computers worldwide in 2003 only $51 billion was legally purchased". The study states that as much as 71\% in Eastern Europe, 63\% in Latin America, 56\% in West Asia and Africa and 53\% in Asia Pacific, of the software installed was pirated while the figures for developed markets of Western Europe was 36\% and North America 23\%.

The computer technology has made it much more easier to pirate the copyrighted works. It becomes very cheap for the pirates to just make large number of copies from the contents of a CD, a song, a movie or a book and sell it at Incomparable rates, thus effectively suffocating the genuine products. Internet makes it even easier since the risks associated with the physical distribution is also eliminated through online distribution. Global networks exist to steal and share protected information including software codes through use of all kind of online communication facilities. These networks do the trick in a very short span of time and then destroy all the traces thereby making any prosecution impossible.

Apart from the software industry, music industry is one of the most affected by the piracy. The very existence of

the legitimate music industry is under threat from the pirated copies and Internet downloads. Even in the case of traditional paper books are copied digitally and distributed thereby reducing the sale of original books.

The Copyright Act, 1957 affords copyright protection in India. As per Section 2 (0), the term 'literary work' includes computer programs, tables and compilations including computer databases. So, copyright violations as well as software piracy can be effectively checked under this Act by instituting a suit for injunctions and damages and accounts of profits, or criminal proceedings under Sections 63-70 of the Act.

There are many international treaties dealing with protection of copyright, as the problem of piracy is not limited to national boundaries. World Intellectual Property Organisation (WIPO) under the aegis of World Trade Organisation is now coordinating all the efforts in the direction of protecting intellectual property rights internationally.

(viii) Economic Espionage

As more and more commercial organisations are depending on computers to store and process data, and on Internet for their communication the scope for economic espionage in the cyber space has widened. Instances of getting the trade secrets of an organisation by hacking their network and selling it or otherwise making it available to their competitors have been reported world over. Some experts say that economic espionage is the
single most important problem, with annual losses of proprietary information in the $60 million range. This is a crime in which both outsiders and insiders of an organisation equally play a role. In some instances it originates with an employee who is in a position to sell trade secrets, and other times the employee is tempted by an outsider to sell the information. In other instances, it may be purely an outside job of a cracker.

(ix) Electronic Money Laundering and Tax Evasion

Money laundering is an illegal activity through which criminal proceeds take on the outward appearance of legitimacy. This process is an unavoidable support system in virtually all profit making criminal activities, as the criminal requires to stash away their ill gotten money and then bring it in circulation after giving it the necessary legitimacy. However it is not easy to do money laundering in the traditional financial system since paper based money transfers always leave a trail.

Thus the criminals, including the international drug peddlers, were forced to use cash in all their transfers across the borders. Using cash to transfer huge amounts was not a very acceptable proposition for them due to the risks involved in such a step, including chances of interception.

32. See also http://rr.sans.org/socai/espionage.php
33. See also http://faculty.ncewe.edu/toconnor/410/cyberspacelaw.htm
In the virtual universe of cyberspace the demand for efficient consumer transactions has lead to the establishment of electronic cash. Electronic cash, or digital money, is an electronic replacement for cash. Digital cash has been defined as a series of numbers that have an intrinsic value in some form of currency. By Using digital cash, actual assets are transferred through digital communications in the form of individually identified representations of bills and coins -similar to serial numbers on hard currency. These computer networks based electronic fund transferring has made transfer of money across the globe much easier and faster. However, this facility has enabled the criminal elements world over, for concealing and transferring the proceeds of their crimes.

An offshoot of the money laundering (including that on the Internet) is tax evasion. Since the ownership of the digital cash or e-cash is not traceable in the normal circumstances, it becomes nearly impossible for the taxman to have a check on the income and expenditures of any individual. Apart from the laundered money, even the legitimate income can be concealed from the eyes of the taxman, to evade the tax thereon.

With these developments in the cyberspace, the traditional anti-money laundering mechanisms and legislations in various countries have become toothless.

34. See R. Mark Bortner "Cyberlaundering: Anonymous Digital Cash and Money Laundering" www.law.miami.edu
Some countries have come up with new legislative responses and many others following the suit. However, development of the informal banking systems and parallel banking in the Internet makes the supervision by central banks less effective, thereby tendering any steps to control tax evasion and money laundering through cyberspace with out much success.

(x) Cyber Squatting

This is a genus of pure cybercrime that has similarities with old strategy of registering trademarks (ghost marks) only to prevent others from using it. Here, the site names in the Internet are blocked and then traded by unscrupulous persons for monetary benefits. Well-known celebrities, commercial and governmental establishments etc are the victims of these activities. USA has passed an Act known as Anticybersquatting Consumer Protection Act, 1999, to deal with this problem. Section 3002 Introduced by this Act amends Section 43 of the Trademark Act of 1946 (15 U.S.C 1125) to introduce civil liability for persons who registers, traffics in, or uses a domain name that –

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of section 706 of title 18, United States Code, or section 220506 of title 36, United States Code.

The Act further prescribes that the offender shall be liable to pay actual damages and profits, or statutory damages in the amount of not less than $1,000 and not more than $100,000 per domain name, as the court considers just.

C. Crimes Affecting National Security

(i) Cyber Terrorism

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe
economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. However, attacks that disrupt nonessential services or that are mainly a costly nuisance would not amount to cyber terrorism\textsuperscript{37}.

With the increase in the role that computer play in all our activities there is a threat of cyber terrorism looming large on the international community and respective national security. Computers today control power delivery, communications, aviation, medical, defence and financial services. They are used to store vital information, from medical records to business plans to criminal records. With all the advantages of using computers for storing and processing data, they have one major disadvantage i.e., they are vulnerable, among others, to deliberate outside attack. 'The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb'.

Terrorists are known to use information technology to formulate plans, raise funds, spread propaganda, and to communicate securely. For example, Ramzi Yousef, mastermind of the first World Trade Center attack, stored detailed plans to destroy United States airliners on encrypted files in his laptop computer\textsuperscript{38}. A website known as the Muslim Hacker's Club\textsuperscript{39} lists tips for things

\textsuperscript{37} On cyber terrorism also see, Dorothy E. Denning George Town university, Cyber Terrorism : http://www.csc.georgetown.edu/~denning/infosec/cyberterror.html
\textsuperscript{38} http://faculty.newc.edu/tocoimor/410/cyberspacelaw.htm.
\textsuperscript{39} http://www.ummalivnet/mlc/hacker.html
such as hacking the Pentagon. A hacker known as Doctor Nuker has been defacing websites for the last five years with anti-American, anti-Israeli, and pro-Bin Laden propaganda.

Today a computer savvy terrorist can play havoc by destroying a computer network in any Organisation. This he can achieve sitting in the relative safety of his home using the Internet and other similar communications systems. He need not even go near the target and put himself in the danger of being caught. The national security consequences of the potential use of the Internet by terrorist organizations have attracted the interest of many academics and government and intelligence officials. As of now the instances of terrorists targeting Internet itself is limited because they are more interested in keeping it alive as they can effectively use it for coordinating their activities and spread their propaganda. There are some instances like 1998 attack on Sri Lankan servers by the Internet Black Tigers, and the Mexican Zapatista movement of the same year, which eventually teamed up with protesters of the World Trade Organization, which gives the glimpse of cyber terrorism's potential. The world is yet to see a significant instance of "cyber terrorism" with respect to widespread disruption of critical infrastructures. However, the FBI and many others, are concerned about the growth of something called hactivism, which is a word that combines hacking and activism\(^{40}\).

\(^{40}\) http://faculty.ncwce.edu/toccomor/410/cyberspace/law.htm
(ii) Cyber Warfare

Another area of concern is the role of computers in a war. The cyber warfare has gained so much favour among the military strategists that most of the Armies world over now have dedicated cyber warfare teams for defensive as well as offensive operations. Cyber espionage to gain the information about the enemy and cyber attacks to immobilise enemy by destroying his information system, and protecting one's own systems from counter-attacks are the twin facets of the cyber warfare. Major public international law questions arise from these developments as to the responsibilities of the nations and their right to retaliate etc.

D. Contents based Crimes

(i) Racial and other hate Propaganda

It is an irony that among those who realised the propaganda potential of the computer networks, at the earliest, where various racial and other hate groups 41. Instances of misuse of computer network by such people were reported as early as 1980s. In USA, Ku Klux Klan, the White Aryan Resistance, Skinheads and other neo-nazi organisations have used the Internet for propagating violence and discrimination against their target groups, usually 'Jews'. With the global spread of

41. See Walker, Clive, P. and Akdeniz, Yaman, "The governance of the Internet in Europe with special reference to illegal and harmful content
the popularity of Internet, the terrorist groups and other extremist groups everywhere, have started using Internet to propagate their hate agenda. The damage is much more than the traditional methods since the reach, speed and secrecy afforded by the net causes greater damage.

(ii) Child Pornography

This is another traditional crime that has gained importance since the advent of the Internet. Paedophiles and child pornography is nothing unknown to the world. But the Internet has made it so easy for the paedophiles to organise and distribute the offensive materials throughout the world\textsuperscript{42}. Also the easy access to unsuspecting children through Internet, to these lurking paedophiles, makes them vulnerable of exploitation.

With more and more schools and homes being connected to the Internet the number of children having access to the net is growing exponentially. One concern of course is that the Internet may allow children unrestricted access to inappropriate materials. Such materials may contain sexually explicit images or descriptions, advocate hate or bigotry, contain graphic violence, or promote drug use or other illegal activities. Since it is easy to befriend a child in any chat room over the net without disclosing the real identity and then to exploit him the Internet has become a very dangerous place for

\textsuperscript{42} See Akdeniz Yaman, "Governance of Pornography of Child Pornography on the Global Internet: A Multi-Layered Approach."
children. In the worst instances, children have become victims of physical molestation and harassment by providing personal information about themselves over the Internet and making contact with strangers. However, it is not advisable to keep them totally away from the net because one of the greatest benefits of the Internet is the access it provides children to things as educational materials, subject matter experts, online friendships, and pen pals. The only way out is proper parental supervision and effective prevention of the misuse of Internet by paedophiles for their nefarious activities.

Many countries have attempted some level of legislative measures to combat this growing menace. For example Section 67 of the Indian Information Technology Act provides that "Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years. and also with fine which may extend to two lakh rupees".
IV. LEGAL REGULATION OF CYBERSPACE

Having accepted that some level of legal regulation is inevitable, at least for the time being, let us now look into the logistics of the problem\(^43\). The real world legal system functions on the basis of certain established assumptions that may not be applicable to the virtual world. So we have to be very clear as to the differences between these two worlds in order to understand the issues and difficulties in establishing real world legal control over the virtual world.

A. Real World and Virtual World

Real world is a physical entity, with well-defined borders dividing it into sovereign States. It functions on the basis of sovereignty of the nation States over its territory and inhabitants. The traditional juristic theory of territorial sovereignty\(^44\), with the King being supreme ruler within the confines of his kingdom, originated as two distinct concepts. The King acknowledged no superior in temporal matters, and within his kingdom the King was emperor. In Roman law it was originally considered that the people had bestowed the emperor's power upon him, but when Rome became a Christian State his power

\(^{43}\) Also see, Wall, David, S. "Policing and the Regulation of Cyberspace", Criminal Law Review special issue "Crime, Criminal Justice and the Internet", (1998): 79-91

\(^{44}\) For details see Dr Noel Cox, The Regulation of Cyberspace and the Loss of National Sovereignty, A Paper presented in the 2002 Annual Conference of Socio-Legal Studies Association, University of Wales Aberystwyth,
was regarded as coming from God. In America also God had been recognized as the source of government, although it is commonly thought in a republican or democratic government "all power is inherent in the people". If the Holy Roman Emperor had legal supremacy within the terrae imperii, the confines of the empire, theories of the sovereignty of kings were not needed, for they had merely de facto power. Sovereignty remained essentially de jure authority. This was not merely power without legitimacy. Medieval jurists cared not whether the emperor had jurisdiction and authority over kings and princes, but focused on his power to usurp the rights of his subjects. Whether this power was de facto or de jure was unimportant.

But to have sovereignty, a state must have a permanent population, it must have a defined territory, it must have a government, and it must have the capacity to enter into diplomatic relations. No other entity could be regarded as a sovereign state, whatever its de facto power. Yet, this definition is increasingly becoming meaningless. The notions of sovereignty and statehood are not easily defined or explained. To a large degree this is because they are principally political concepts, rather than merely legal principles. With the growth in both the (horizontal) extent and (vertical) reach of international agreements, treaties, conventions and codes, national independence is becoming

45. P. Canning, Law, sovereignty and corporation theory, 1300-1450, in J.H. Burns (ed.), The Cambridge History of Medieval Political Thought, Cambridge University Press,
46. Kenneth Pennington, The Prince and the Law, University of California Press, Berkeley,
less relevant. This tendency is becoming more noticeable in the modern commercial environment, and especially the Internet.  

The virtual world confirms to none of the accepted requirements of the sovereignty. Cyberspace does not have a permanent population, it definitely has no territory, it has no government, and it has no capacity to enter into diplomatic relations. Therefore, the very concept of sovereignty is not amenable to the virtual world called cyberspace. Persons enter the digital world by going online and come out of it by merely disconnecting. No one is a permanent member there and anyone can enter it at a given time provided he has access to it through connectivity. It has no centralised authority controlling its affairs. Even the largest regulatory body in the Internet, ICANN, has a very limited role of allocating and regulating domain names and no other control over the activities of the Net. These fundamental differences from the real world make cyberspace not an easy entity to regulate, because the real world regulations functions, as already mentioned, on the basis of certain established assumptions.

V. LEGAL REGULATION IN REAL WORLD

A. Geographical Determinacy

The sovereignty based nation-state theory recognises law-making power as a state's prerogative. The positivist school of jurisprudence, while reaffirming this line of thinking, signifies that the State's sovereignty as the source of law. Therefore, generally all laws are State specific. Only notable exceptions are the slowly but steadily expanding horizons of the international laws, both public as well as private international laws. Even in the case of these exceptions, the source of legitimacy is accorded through the sovereign's treaty making powers. This sovereign power to make laws is always circumscribed to a determinable geographical territory.

B. Territorial Enforcement

A positive law in the real world, originating from a competent sovereign authority, is entitled to be enforced in a given territory where the power of sovereign runs through. This principle of territoriality is generally accepted in the sphere of criminal

jurisdiction. The principle is based on mutual respect of sovereign equality between States and is linked with the principle of non-intervention in the affairs and exclusive domain of other states. These principles of comity and non-intervention impose limitation upon nation States in applying extra-territorial criminal jurisdiction over the subjects of or activities in another sovereign State.

The offshoot of this principle is that in-ease a State wants to enforce a particular sovereign law beyond its determined geographical territory, and try a citizen of another State, it has to obtain the sanction of municipal court of the other state to get the accused extradited. Criminal prosecution generally requires the physical presence of the accused.

C. Notion of Property

Traditionally, the real world legal systems construes property as some thing perceivable, tangible and objective. A notable exception to this general assumption was the intellectual properties. Even in the case of intellectual properties, the property rights in them are normally associated with physical manifestations of the intellectual property. Thus the principles of traditional legal systems find it difficult to adjust to the notion of digital or incorporeal property. For example the

traditional laws dealing with theft may not be effective where a hacker steals a password of a computer system\textsuperscript{51}.

D. Paper Based Transactions

In the real world, the law always encourages people to enter into legal relationships by reducing the relevant terms and conditions in writing in a document\textsuperscript{52}. In the cyber context however, the emphasis is just the opposite; it encourages paperless transactions. It substitutes paper with electronic or digital records.

E. Real Relationships

In the real world, the physical relationships between the persons are of the essence in any transactions, be it a marriage\textsuperscript{53}, or contract\textsuperscript{54} or offence of murder\textsuperscript{55}. The traditional legal systems thus find themselves not equipped to deal with increasing trend of virtual relationships that are emerging in the cyberspace.

\textsuperscript{51} See the case study related to Love Bug Trial in Philippines.
\textsuperscript{53} See Section 5 of Hindu Marriage Act, 1955
\textsuperscript{54} Section 2 (h) and 10 of Indian Contract Act, 1872
\textsuperscript{55} Section 300 of Indian Penal Code, 1860
VI. Legal Regulation in Cyber World

We have already seen that cyberspace is not amenable to the traditional notion of sovereignty, which is based on the determinable territorial limits and nation States. So, let us now analyse as to what are the implications of invoking the above real world assumptions in the context of legal regulation of cyberspace\textsuperscript{56}.

A. World without Boundaries

Cyberspace does not recognise any boundaries\textsuperscript{57}. According to William Gibson, the science fiction writer, who supposedly coined the term "cyberspace" it is the space between two modems. In other words, cyberspace is where the Internet is located. This electronic realm does not occupy any corporeal area, except perhaps to the extent that it relies on hardware such as computer equipment and telephone wires. It is a virtual world existing only through electronic pulses. The Internet, which constitutes the major share of cyberspace activities, does not function like other communication channels that establish a continuous tie-up over the entire channel between two people who are using it. In Internet, the information is broken into


\textsuperscript{57} Jonathan Rosenoer, "Multistate Compliance: Are You Ready to do Business on the Internet?", WIRED 5.03 (1997)
discrete packets of bits that can be transmitted as capacity allows. Packets are labeled with the address of their final destination, and may follow any of a number of different routes from Computer to computer until finally reaching their final destination, where the recipient machine reassembles them. Thus, packets from a variety of sources may share the same channel as bandwidth allows\textsuperscript{58}.

Since the Internet uses the packet system that may use numerous nodes situated in different continents to route some information, only on the basis of availability of the interconnections at that point in time, the borders between countries involved loses their significance. No single country can claim an activity took place in its entirety within its borders and thus in its jurisdiction. Political State boundaries are not relevant to the cyber criminal who deals in the commodity of information\textsuperscript{59}. Intervention and State regulation cannot form successful barriers against a good that is by nature an intangible resource which cannot be stopped at the customs border or contained within a specific geographical area. Information can be exported from one part of the globe, where it might not necessarily be illegal, to a state where the possession of such data is criminal. Likewise, through electronic bulletin boards and web pages, parties can discuss ideas or import {download} information without hindrance from state authorities\textsuperscript{60}.

\textsuperscript{58} Dan L Burk, Jurisdiction in a World without Borders, 1 Va. J.L. & Techo 3 (Spring 1997)http://vjolt.student.virginia.edu
\textsuperscript{59} Timothy W. Luke, "Simulated Sovereignty, Telematic Territoriality:
\textsuperscript{60} Juliet M. Oberding, A Separate Jurisdiction For Cyberspace
B. Enforcement cannot be Territorial but Global

Since the territorial borders have no relevancy in the cyberspace its activities can not be subjected to anyone particular jurisdiction with legal justification. The offender might by sitting in one country and using a system situated in another country might commit a crime in a third country. Even in such relatively simple situations, number of countries involved may be much more since the transaction was accomplished, by information flows through various other countries, without the knowledge of the offender. The legal responses in each of these countries could vary and the jurisdiction of one particular country may depend on the legal system that is followed therein. Even when a particular country assumes jurisdiction and set out to prosecute the offender, issues like investigating the crime, collecting evidence from systems located in other countries and procuring the offender's presence to stand trial etc poses problems.

In order to overcome these problems, the only solution is to ensure that the enforcement is not territorial but global. The States must

cooperate and coordinate in their activities, in regulating the cyberspace. The ultimate objective of all efforts in combating crime in cyberspace must be to evolve an enforcement regime that is based on globally accepted principles.

C. Property is Notional

Traditional notion of corporeal property cannot be adhered to in the cyberspace. Here the property is notional. Although protection for information and other intangible things or values existed before the middle of the twentieth century, it did not play an important role until very recently. A new doctrine of criminal information is emerging in the area of legal science, founded on the still developing concepts of information law and the law of information technology. In accordance with modern cybernetics and informatics, information laws now recognise information as a third fundamental factor in addition to matter and energy. This concept evaluates information both as a new economic, cultural and political asset and as being specifically vulnerable to unique forms of crime66.

It is obvious that in this new approach, legal evaluation of corporeal objects differs considerably from the evaluation of incorporeal (information) objects. Firstly, there is an important distinction

between information and data that is both technologically and legally relevant. Information is a process or relationship that occurs between a person's mind and a stimulus. Data, whether in corporeal or incorporeal (e.g. electromagnetic impulse) form, constitute a stimulus. Data are merely a representation of information or of some concept. Information is the interpretation that an observer applies to the data. Thus when data are destroyed or appropriated, it is the representation that is destroyed or appropriated and not the actual information, idea or knowledge. The latter may still subsist in a person's mind or in another copy of the data. Second difference concerns the protection of the proprietor or holder of corporeal and incorporeal objects. Whereas corporeal objects are more exclusively attributed to data that flows freely in a free society, it is not itself subject, therefore, to exclusive protection in the same way as tangible property. A third difference is that while protecting information not only one consider the economic interests of its proprietor or holder, but one must also preserve the interests of those persons concerned with the contents of the information. This aspect forms the basis of privacy protection.\(^{67}\)

In the cyber world the property is of notional value and information form the core of the property. Particularly, domain names, content of the web pages and graphic designs form part of the proprietorship of the cyberspace.

---

\(^{67}\) Ibid
D. Virtual Relationships

Because of the connectivity, speed and accuracy as to transmission, the interactions in the cyberspace acquire distinction of virtual character. The Internet offers anonymity; unless one volunteers information about self, the opposite party has no means to identify as to whom he is dealing with. Even the location of the opposite party is not identifiable over the Net. These characteristics render virtuality to the relationships formed in the cyberspace and make it more complicated for the traditional legal systems to deal with.

E. Digitised Records

In the real world the transactions generally leave some sort of physical evidence in the form of things or records. In the cyber world such records might exist only in a digital form. Even this digital information may reside partly in number of computers and formed into single record only by the processing of a computer. That means, unlike in the real world transactions, finding out evidences of the virtual transactions will be cumbersome since the same may have to be reconstructed form the bites of information contained in many systems. Also the difficulty arises as to proving the authenticity of digitised records, as they are susceptible to changes easily. Many of the nations of the world have legislated to overcome these problems and given legal recognition to technology based measures in authenticating digital records.