Legal control is the most effective means to control crime in society. The other means are social consciousness, economic reform, moral education etc. Our study relates to the legal control of cyber crimes, a new member to the family of criminal wrongs. Criminal science, of which criminal law is a part, deals with the criminal, causes of crimes, criminal policy of the government and the enacted laws, also the universal rules and principles, including the substantive and procedural laws as a whole. And hence the legal control has been most effective and scientific onus.

Managing cyber crimes involves a concept on cyber crime, and the cyber space and also the working of the traditional crime management system. Cyber crime has been defined as the crime involving computer and communication system or the Internet. And it also means the application of some knowledge in digital technology “Computer crime has been broadly defined as any illegal act that involves a computer, its’ systems or its’ applications.... The United States Department of Justice provides another definition, stating that computer crime is any illegal act for which knowledge of computer technology is essential for either its’ perpetration investigation or prosecution”. * 1 Essentially these crimes some how involve the Internet or cyber space so in a sense the cyber crime is the illegal activities in the cyber space.

The technical space commonly called CYBER-SPACE is the product of human intellect, wisdom and perseverance and it ultimately frees the human being from the age old concept of territorial authority hegemony and control mostly led by the ruling powers. From the year 1989-1995 onward the cyber space has been a new territory gifted by the science and technology and hence this territory requires both governance maintenance, improvement and also the law enforcing mechanism to control restrain and coerce the irregular injurious and willful deliberate violations of fair use code of conduct policies and rules.

The threat of cyber crimes may also be, to some extent, controlled and checked by technical means like employing devices (Firewalls), regular security checking (by scanners), restricting physical access to the computer computer systems or computer network etc. The Defence Information System Agency (DISA) conducted a long series of test Hacking (Circumvention) on Department of Defence Networks in 1994 through 1996. The Hack attacks were friendly but to search for loopholes in the DOD networks using Hacking tools commonly available in the Internet.

Table – 5 * 1A

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No of Networks (DOD) attacked</td>
</tr>
<tr>
<td>2</td>
<td>Successful penetration &amp; taking control</td>
</tr>
<tr>
<td>3</td>
<td>Detection by Network Administrator</td>
</tr>
<tr>
<td>4</td>
<td>Detection</td>
</tr>
<tr>
<td>5</td>
<td>Reporting</td>
</tr>
</tbody>
</table>

* A * Infra 20 ------ Cyber Shock ------- 2000 -- --------------- P - 20
This work focuses only on the group of offending activities marked as cyber-crimes, which need separate legal treatment other than wrongs marked as civil wrongs. This work further excludes the damaging and destructive activities involving Internet channel carried on by or on behalf of International Terrorist groups, and also excludes those arising out of inter state rivalry of enmity among nations or cyber warfare.

Here the legal control means and includes detection reporting investigation prosecution trial and conviction. "since the vast majority of cases are resolved prior trial many of the reports of these cases are available only as news stories rather than in the form of court decision." * 1AA

So legal control involves all the security incidents/which are resolved prior to trial (2) which are compounded during trial (3) which are dropped by the prosecution for any reason. (4) where the prosecution fails to prove the offence charged (5) where the prosecution leads to conviction.

5.1.1. –

A CONCEPT OF CYBER CRIME

CYBER CRIME is the new member of the family of criminal law but unlike white collar crime it has gained very fast recognition demanding immediate attention follow-up and combat. And much before the legislature and judiciary, the law enforcing authorities had to face this new traditional weapon like firearms could be useful to face cyber criminals.

The concept of cyber-crime has been generally described as the wrongful and immoral activities by human being and these activities partly or fully take place in the electronic media. The electronic media is comprised of the information network or the Internet and the online computer. "Some cyber crimes reach a very where and hurt everyone. Electronic commerce crime, (like the theft of hundreds of thousands of credit card records) threatens the Internet boom. Economic espionage (like the theft of biotech secrets stored in digital files)....Infrastructure attacks (like an assault against a nation’s power grid) threatens the safety and well-being of whole populations. Other cyber crimes, such as identity theft or cyber stalking, strike at netizens, exposing them to financial psychological and even physical harm" *2 In the same way as the traditional criminal science of real space. The cyber crimes have been separated from other wrongs in the cyber space by a vague and fluctuating line. And the principles of criminal liability like mens rea have remained important guideline generally with often creation of statutory offences grossly violating the scientific principles of criminal liability. The individual items of the offending activities in the cyber life like unauthorized access or hacking, theft of proprietary information like ID card number, password or trade secret, financial fraud through cyber space, injecting malicious code or virus, into the Internet, disruption of network traffic by denial of service attack, software piracy and copyright violations, false domain name registration, spamming the junk-e-mails, spoofing or forged e-mail and like many others, have been classified into civil and criminal wrongs.

But this classification has been made differently by different municipal governments without any uniform criminal policy throughout the world, nor does it follow any scientific rule of criminal liability. "In cyberspace, there are not only no national or local boundaries to contain the scene of a crime and determine the method of its’ prosecution, there are no clear cultural agreements on what a crime might be....."3

1AA*Sup-1--- 2001 ---------p --304
The mode of cyber-crime is very much different from that of the real space crime in many ways. All the features of traditional crimes namely human being act or omission, intention and injury are present in cyber offences but the interconnection as among these are remote and highly technical. Malicious act committed in one country can cause injury or damage in another country but the injury remain invisible in some cases till the victim checks his database or materials placed on-line. And the relation between the act committed and the person committing is too weak to detect, to identify and to locate by the LEA. The common instruments of house breaking, fire arms weapons usually employed by criminals are not used by cyber criminals. Thus the new space of electronic world has necessitated its own instruments and mode of commission “ICTs are making possible both new ways to commit crimes as well as new crimes themselves.” *4

In cyber world- hacking and cracking are very prominent criminal activities causing serious security problem to all concerned. Hacking means unauthorised access in the computer’s database and cracking is the hacking with malicious intent. Every host computer (i.e. physically connected to the Internet cabling) has a particular IP address code and thus it can be reached in the normal course Internet searching. And the WWW system has easier to remember and use the address code for any online database. “Computer crimes are made possible the combination of computers with telecommunication abilities. The power to send data over communications equipment has transformed our society completely.” *5 The opening of the private or protected part of the database is actual operation done by the hackers. The private database is protected by several means like password, encryption and firewalls and the like. And the hacker then applies his personal knowledge, painful trial and error method; technical knowledge used in phone hacking (phreaks) some tools like password breaker etc. And ultimately the hacker becomes successful to open the protected database and then he collects it or store it in another computer’s database. (Which has been captured in the same way beyond the knowledge of the real user or owner).

And again the hacker may not directly operate from his own computer but he first enters another soft-target computer and captures it and then employs it to reach the real reassures or rich target. This known as looping is done to camouflage his identity and to mislead the investigator. And it is difficult to trace any evidence or materials as are materials, commonly used in traditional crime investigation. And once the hacker gets into the database by discovering the password or encryption-code or another protecting and device he technically captures the machine and operate that victim computer interactively i.e. he can add, delete, modify, erase the entire materials therein.

The virus dropping in the communication network has been observed to be much easier than hacking. The computer virus (dormant) and worm (active) are nothing but sets of instruction code written in machine’s language. Thus virus can be kept hidden in a file and it becomes active to infect others files and multiply when the infected file is opened and run. But the worm can be injected into the communication line through a simple e-mail from any cyber-café or PC online. The worm reaches one or more computers and creates anomalous activities in the computer working leading to its crash or breakdown and in the mean time the worm passes to other innocent computer, computer system or computer network and in this way paralyses, dislocates whole region until some defensive steps are taken. The cyber-hackers are proud descendants of phone hackers or phreaks. Phreaks could capture telecommunication line (PSTN) through the automatic switching center by applying their knowledge, experience perseverance, trial and error method, and using some tools like blue-boxes, tuning devices to create tones and sounds of specific frequencies (tones and notes) etc.

4* D.Thomas & B.D.Loader – Cyber Crime ----2000-------Routledge NY------P---103
5* sup-1-------- 2001----- p-298
The cyber hackers thereupon have successfully improved their capabilities to capture targets computers and to keep it under his control in a way inaccessible to other “Hackers use encryption to protect their communications on Internet Relay Chat (IRC) Channels from interception. They also have installed their own encryption software on computers they have penetrated. The software is then used to set up a secure channel between the hacker’s PC and the compromised machine. This has complicated but not precluded, investigations”. *6 And various other types of offending activities like creation storing and transmission of porn-materials, on-line gambling cyber-extortion (Bill Gates case-spring 1997), theft of vital records, data fraudulent commercial activities. Intellectual property offences, and so many other offences are committed involving cyber space and high technical knowledge and each of these has its own mode peculiar to its' purpose and target of attack. The mode also changes with the gradual improvements in defensive methods employed by the netizens, law enforcing authorities and the different hard ware and software innovations.

The definition and concept of computer crime has been further complicated by the advent of the Internet, “prior to the Internet and computer networks, the number and variety of computer crimes were extremely limited. Such crimes usually consisted of illegal acts such as computer trespass and data manipulation or destruction.” *7 But after the Internet many more items have been added to this class of wrong. These are system penetration by hackers, theft of proprietary information, financial fraud, disruption of network traffic, (Denial of service attack) sabotage of data network distribution of computer virus Trojan horse etc. software piracy, and intellectual property right violations in cyber space.

History of cyber crime may be said to have been started in 1960s before which stand - alone main frames (big computers) were very costly (millions of dollars) and very few in number and were kept under strict control of technical expert groups. “In the 1960s, the term hacker were used to refer to someone who was considered a ‘real programmer, who had mastered the computer systems of the day and was able to manipulate programs to do more than they were very originally intended to do”. *8 In the 1970s phone hackers or phreaks were active to access phone networks. These phreaks gaining more knowledge turned towards computer networks in 1980s and 1990s. Long distance telecommunication network were accessed to commit bank transfers (Vladimir Levin) and disruption to the services. They are not actually Internet hackers but advanced groups of them. But hacking in present concept is an act of intrusion with ill motive. “Law Commission in England recommended that hacking be made penal. It says the main argument the in favour of hacking offence does not turn on the protection of information but rather springs from the need to the protect the integrity and security of computer system from attacks from unauthorized persons seeking to enter these systems, what ever may be their intention or motive”. *9 Along with hackers the creation and distribution of malicious codes became another mode of cyber-crimc. “The first viruses were developed in the early 1980s. The first viruses were found ‘in the wild’ were apple II viruses such as ELK cloner, which was reported in 1981.”*10 Various other virus were created in subsequent years such as Brain virus in 1986.

---

6* Supra -------4-------2000------p------107
7* sup-l ------- 2001-------- 300
8* Atul Jain Cyber Crime - Issues Threats and Management (vol-II) –2005
   Isha Books Delhi- p-61
9* Yatindra Singh - J I L I- 2002—vol-44—No.2—p—197
10* sup-8 vol-I ---------------2005----------p-55
Almeda in 1987. Another code Christmas tree worm which if executed would display an Xmas tree and would send a copy to everyone on user’s address list. The famous Internet worm was created by Robert T Morris, a student of Cornell University in 1988 and it went out of his control and damaged thousands of computer and slowed down the Internet. He was however then arrested and punished.

Thereafter many other Internet worms (malicious codes) have been created in many cases, the author could not be traced and punished such as the authors of code Red worm of 2001 July 19 and NIMDA of 18 September 2001. “The advent of network computers has created unprecedented opportunities for the anonymous perpetration of crimes. Computers as the target of crime, as a Tool in the commission of a crime as Incidental to a crime.”*11. The different forms or name of cyber crime, which we find to day, are not small in number and new varieties are added day by day. However these may be classified in three broad groups (a) crimes against persons or business (b) crime against property- tangible or intangible (c) crime against Government. Some of these are hacking, cracking, malware (Virus, Trojan horse worms, Logic bombs), Denial of service, pornography, stalking, fraud, gambling, spamming, commercial espionage, privacy (software and Hardware) disruption to health, safety, essential service, espionage Terrorism, & Intellectual property crimes.

5.2.1 DIFFERENT TYPES OF CRIMES AND MODUS OPERANDI

The dark side of cyber space has some difference from the real space in that the offenders here employ high-tech means to commit crime and very often remain anonymous. The anonymity has been a very great advantage perhaps for the ill motivate persons in cyber activities. “Computer crimes may just be high-tech variations of conventional crimes and consist of traditional crimes committed with the help of the computers, such as distribution of pornography. Other crimes are solely the product of phenomenon of the Internet.”* 12 The Internet has provided some special advantages to ill motivated persons such as remote activity, jurisdictional jump, encryption, easy and instantaneous actions etc. some of the new crimes peculiar to the Internet are Net Work attacks, sabotage of data, malicious codes (Virus, worm, Trojan horses) Web defacement. And some of the traditional crimes have been modified in the cyber environment computer related fraud, theft and extortion, pornography, gambling harassment (cyber stalking), violation of intellectual property right. “ The kinds of crime instigated on Net are indeed many and varied. Some of the most common would include the following: Computer network break in s. industrial espionage ............... software piracy”. *13 Cyber squatting – panavision – vs – Toeppen – 938. F.Supp.616 (C.D. Cal. 1996) – reserving and then reselling domain names.

The most Important crimes however relate to the unauthorized access and damage to the networks and on-line computers by criminal hackers, some other like virus and worms. Denial of service attacks (DOS), spamming (…e-mail in huge volume), pornographic materials etc.
5.2.1(a)

**HACKING**

The idea of cyber crime has, in many ways, become synonymous with hackers and hacking.

Douglas Thomas.

Hackers are the most dignified and talented offenders in the cyber space. Literally hacking means to strike or to cut something. In the virtual world the hacker means a person taking backdoor access in a computer’s database or resources with or without any ill motive to cause any damage or injury to the computer or computer network.

"The highest risk that the information technology business faces to day is the security of information in terms of integrity, availability and confidentiality ....... Today, all system intrusions and virus attacks point to a community called hackers ........ in general terms, hackers are individuals who break into information systems. However, all hackers are not harmful to information security." *14 Hackers take the advantage of any loop-hole or weak spot in the computer program, security provisions or technical vulnerabilities. And for this reason, a hacker must have sound knowledge in computer mechanism, programming, software applications and network-technicalities.

**INTRODUCTION TO HACKING**

**Early Hacking(1)**

In the 1950s when the electronic computer for the first time became available to private people, the user community was very limited due to its very high cost and were used for the research work and for very limited commercial jobs and the defence areas. So the access to the electronic machine was naturally very restricted and non-users had little chance to use or to make any abuse to derive illegal gains.

In the early stage i.e. 1950s. hacking denoted extra-ordinary method to run the machine and get it worked. “However, the prime aim of those hackers was to experiment with new solutions without any malicious intent”. *15.

A new stage in computer use and operation arose in 1960s when time sharing system was developed. The time-sharing system introduced the rules of using logon names and passwords. “The hurdle of logon names and passwords redirected the activities of hackers from merely performing experiments to trying to find out those logon names and passwords. Hackers tried to guess the logon names and passwords of legitimate users” *16 The hackers in this age tried to guess the logon names and passwords from the first names, last names, names related to the family of users etc. and sometimes they are successful to guess the correct one (logon names/passwords) and break into the computer or time sharing systems.

In the mean time in 19th century railroad had been leased to Telegraph Companies and again it was taken by telephone companies to developed long distance network. “The telephone system was the first global computer and it was legitimate political target”. *16 A The global telephone network had provided for teleabuse and telephone hacking called phreaking in the early second half of 20th century.

---

14* NIIT Ltd.- Hacking- Tools & Technique- 2003-Prentice Hall of India New Delhi-P-1  
15* Sup- 14--- 2003----------P-(3)  
16* Sup ----14-------2003----------P----3  
“In parallel to the computer hacking activities a new type of hackers, phreaks came into action. Phreaks first accessed telephone networks by using handheld electronic devices. Phreaks used those devices to make modifications to pay-telephones to make free telephone calls. To emulate payments in pay telephone they used devices, such as red boxes. Later new and sophisticated devices, such as blue boxes were introduced. Red boxes and blue boxes are electronic devices used to transmit digital sounds and tones over a telephone network. In the early days of phreaking, phreaks used these boxes to access telephone networks with the privileges of telephone operator.”*17

Stewart Nelson, a MIT student and a Phreaker, used computer generate suitable tones to access long distance phone service. Some Phreakers used toy whistle and / or even own voice to make and apply suitable tones to access phone system, generally Phreakers used blue box tone generators to produce 2600 HZ tones for breaking into phone system. However this (frequency) tones were abandoned by the phone-companies thereafter. “John Draper, a US Air Force veteran and engineering technician for Nation Semiconductor who went by the alias of Capt’n Crunch, is generally credited with designing the original blue box, that granted access to AT & T’s long distance service”*18 John Draper, however arrested in 1972 for making and supplying blue boxes but he is said to train Phreakers and hackers while in prison also.

He had close nexus with the then Phreaker and hacker community in USA. Steve Wozniak the inventor entrepreneur of Apple Computer Company was one of the hacker associates of John Draper.

The British Telephone network had its Phreaker counterparts in England in 1960s and 1970s to make free long distance calls, and to take other advantages. They developed Bleeper Box to create deceptive tones of variable frequencies like the Blue Box of John Draper to take backdoor access to the phone-network.

“In addition to the original blue box, Phreaker constructed a number of other devices to outwit the phone system. The red-box replicates the tones that are produced when coins are deposited in a pay phone and a black box allows calls placed to the phone to which it is attached to be made free of charge. Manipulation of the phone system was also popular with people engaged in other criminal activities, to cover their tracks......... The ‘chess box’ was devised to connect two lines at a location in such a way as to allow bookies or drug dealers receive calls from another remote location and go through the chess box to disguise the number at which they were actually located.”*19

The global telephone network thus provided the training and breeding for the computer network hackers of the next decades “over the years, older analog telephone equipment has been replaced with digital computer equipment and Blue Boxes don’t work much any more. As the older equipment was being replaced with digital equipment, computers were playing a larger role in controlling and switching calls, as well as in maintenance work. Computers allow all the new services, like caller ID. Conference calls and other features, which were hard to implement on mechanical switches..... the phone companies installed remote access to the switches, a

16* sup-14---------------------2003-------------------------p3
17* sup-14---------------------2003-------------------------p-4
18* sup-8----------------------V-II-----------------------2005---p-63
19* sup -8 ----------------------V-II ---------------2005---P--64
Security problem of course, all transaction with the computer are logged, but hackers have ways of hiding their activities --- In the last thirty years, phone hacking (preaking) has merged with computer hacking .... There is a much greater variety of things hackers can do now. More equipment and software means there are so many more hackers needed to get in to systems. But, because most of this equipment can be purchased through independent companies it is easy for a hacker to pose as customer..... ‘John Cap’n Crunch’ Draper- December 1999” *20

In the new age of computer telecommunication, the phone hackers equipped themselves with the knowledge of digital technology “ B B Nanda and Dr. R. K. Tiwari observe that ‘internet paedophilia computer network breakins, industrial espionage fraud, software piracy e-mail bombing and spamming and the availability of illicit or unlicensed products and services are already making themselves felt.”

MODERN HACKING II

Hacking as we understand today in the 1st decade of 21st Century is a combination of the 1st age hack experiments on stand-alone computers in the 1950s .......... Then the telephone hacking or phreakings in the 1960s and 1970s and also the hacking in the computer telecommunication systems in the 1980s and 1990s. And in this view the present hackers we may call the 4th generation, hackers have been enriched by previous experiences and intensive practice, dedication and devotion and mutual exchanges of knowledge on technical issue. “Hackers spend months and years learning about computers, operating systems, networks, programming and software. The image of colourfully creative coifs, painful piercing and poorly dressed drinking gallons of Jolt Cola, absentmindedly munching on pizza and conducting marathon hacking sessions for twenty-four to thirty six or more hours is not too far from truth.

That is the dedication required to get inside the mind of the computer, know the nuances of the network and have the personal wherewithal and stamina to continue despite failure after failure. Because at the point the skilled hacker will prevail and the network will be his.

The truly skilled creative and original hacker will spend his every available working moment in the pursuit of knowledge and access to computers no matters his true motives. He will learn from his mistakes be cautious in his endeavours and perfect his techniques. Perhaps he will build better hacking tools to speed up his tasks, automate the redundant steps and build alternatives for attacking different kinds of computers.

*20* Winn Schwartau- Cyber shock—2000—Thunders Mouth Press NY-Foreword (XVI)
And all of this takes time a lot of time. Many hackers today spend countless hours looking for weaknesses and vulnerabilities in computer operating systems like Windows-98, NT or the many flavors of Unix. Others will acquire software programming, take errors that they can exploit. *22

In addition to personal training and study, they participate in Bulletin Board Service or Conferencing to exchange news and views on technical issues, they also maintain websites and other quasi legal activities in the cyber-medium. These websites provide hacking tools (software) to the intending users also over the Internet. *22 Attackers require less knowledge as tool sophistication increases. The sophistication of the hacker has gone consistently down since the early 1980s. To day push-button hacking can make anyone with a modern and an attitude a royal pain in the patoot. It’s only going to get worse before it gets any better. *23

The attack tools thus are being refined to make it easy to use by hackers starting from password guessing in 1980s, then password cracking. Exploiting known vulnerabilities, disabling audits, backdoors, hijacking sessions, sweepers, sniffers, packet spoofing, and tools with GUI etc in late 1990s.

**Some hackers sites** : http://hackernews.com
http://www.2600.com ; http://www.2QitO.com
http : hackingsecrets.com
http : www.hcktik.com
http : www.attrition.org
http : www.undergroundnews.com
http : www.hacker.org
http : www.kevinmitnick.com
http : www.technotronic.com
http : www.insecure.org
http : www.phreak.com
http : www.defcon-org/http://www.hogus.net/kiyc
http : www.rsa.com
http : www.ucl.ru
http : www.cyberstalkers.org
http : www.comperna.ru/famous/hackers

Hacking in the computer-telecommunication was different from Internet hacking in the sense that in telecommunication system the attack route remains the same during same operations.

Hacking as a technical know how is not illegal so long it is within the limit of authorization i.e. for security testing auditing or vulnerability assessment and also for academic purpose or training purpose subject to the hacker’s own or permitted sites.

“And now a days the media has been wrongly and outrageously referring to computer criminals as Hackers. They fell to recognize the fact that criminals and hackers are two distinct terms and are not associated with each other whatsoever. People have wrong notions and for reasons not justified at all they have negative attitude and utter dislike for ‘Hackers’ and persons associated with “Hacking”. *24

---

22* sup—20--------2000--------p-7
23* sup—20--------2000--------p-42
24* Ankit Fadia—Un official guide to ethical Hacking – 2001 – Macmillian India Ltd. ND – Preface
In practice hacking is technical know-how and expertise, a branch of ICT but quite reasonably may be exploited by criminals as well.

The computer managed telecommunication system in 1970s on-wards gave the long arms to the hacking community. In 1970 Carlos Salgado (a.k.a. SMAK) of California hacked several media companies like world wide web and some ISPs. He accessed the huge databases of the media companies exploiting the flaws in the operating systems and using commonly available hacking tools and managed sixty thousand of credit card records there from.

"The details of Salgado's digital adventures and the FBI investigation that brought him to justice provide a fascinating and invaluable glimpse into the shadows of cyber-space and shed light on the dark side of the electronic commerce gold rush..." *25

The investigation of this case provided the valuable information for all cyber security incidents. On 28th March 1997 one ISP technician at San Diego noticed unauthorized access and also a packet sniffer placed in the system to collect logons. The technicians at once backed up relevant files. The access was traced to the University of California at San Francisco.

The FBI on investigation discovered that the unauthorized access into the ISP's system actually came through an account of a student quite ignorant of the situation. And ultimately carlos SMAK was arrested with the CD-Rom containing about 1 Lac credit cards numbers in the San Francisco airport in 1997.

Chris Goggans (aka Erik Bloodaxe) in 1990s became notorious hackers and founded the hacking group Legion of Doom (LOD). The member hackers of the LOD were engaged in criminal activities in exchange of money or as hacker for hire. However Chris Goggans could not be arrested and prosecuted on the charge of hack ---- attack on any computer network. But for any reason, Chris ultimately changed his mind and gave up criminal hacking and became a computer security professional in late 1990s. Serej Goyarchuk (19) a student broke in several mailboxes of corporate bodies and of some private e-mail users in Russia. He was prosecuted and convicted accordingly.

In 1998 September one hacker Ilya Gofman (2) alias spy-Bull a student in Moscow managed a large sum (about $20,000) from one E-zine in USA And transferred to an account in Moscow. The concerned account holder cashed it and passed it to spy Bull. However Gofman was identified prosecuted and punished in Moscow. Andrej Leshutin (alias-Leshy), a Russian cracker was arrested in late 1990s by the cyber police (http://www.cyberpolice.ru). "Lashy is said to be accused of fabricating (and disturbing) computer infections. This news was met with fierce disapproval by numerous members of the hackers community and the lively discussion has been removed from the website guest book to the specially organized forum (http://www.computera.ru/forum/hackers). While the discussion proceeds, highly critical views are being addressed to the security and cyber police bureaux." *26

Hackers usually prefer to form small groups and individual hackers are generally uncommon. One such Russian group RAF (Russian Anti Fascist Frontier) generally engaged in spreading and upholding political views rather than, committing criminal activities. But another group RSA (http://www.rsa.com) is engaged in offensive and illegal activities and they invite others to join them and set a target system to be cracked to win a prize. Another such team is Hacker zone (http://www.hackerzone.ru) which functions in close collaboration with a German team 'Werwolf' (www.werwolf.de)
The United Crackers League (UCL- http://www.ucl.ru) was also engaged in criminal activity where the above mentioned hacker Leshy was an active member. But the team suo motu changed their course of action in 1999 and stopped criminal activities. "Not all hackers bore malicious intent toward the system they infiltrated. Largely harmless pranksters of the old school continued the hack along with young turks who were bent on causing as much cyber havoc as possible.

Yet another style of hacker was emerging like their predecessors, these new hackers strove to remain anonymous. Quite unlike those who had gone before, they did not seek to attention to their activities. Rather they wanted to remain unobserved as well as anonymous, because detection would mean their routes into a system would be closed. This new breed of hacker broke into systems to use them and/or to view data they stored. This meant they weren't in their ripping up databases. Thus the likelihood of detection was less, and this short of hacker's instructions could and did continue for months on end". *27 Sometimes hacker use virus as a tool to dislocate the function of a computer or computer system. And in this method the hacker in most Cass remain untraced. "The Hacking group ‘Cult of the Dead Cow’ releases its’ Trojan Horse program, tool at Def. Con Once a hacker installs the Trojan horse on a machine running Windows 95/98, the program allows unauthorized remote access of the machine." *28

The hackers exchange their views and share knowledge among them selves and hence they run their own websites and attend conferences. They protect their own websites from being attacked by others and LEAs.

Some of the hackers websites :-
http://hackersnews.com
http://www.2600.com
http://www.hackingsecret.com
http://www.telchack.net
http://www.hackzone.ru

The hacking tools (software) are easily available in the Internet website and hence these are downloaded and used.

SECURITY SITES
There are some sites providing assistance and guidance in need against criminal activities in cyberspace.
http://www.infowar.com
http://csrch.nist.gov/
http://www.cart.org/
http://www.microsoft.com/security/
http://www.sans.org

Hacking Laws...... III

The United States enacted the law on (1) Fraud and related activity in connection with access device u/s 1029 which prohibits possession production or transfer of access device to be used in telecommunication lines . The Act provides for a penalty of fine of imprisonment of ten years of both .(2) Fraud and related activity in connection with computers u/s 1020 (a) (1) and (2) relating -------

26* sup -4-------------------------------2000-------------------p--65
28* sup -8--------------------------vol-----1------2005----------------p--60
to unauthorized access and obtaining the information there from. The penalty for non-
government computer access is fine or imprisonment for one year or both. But for
government computer access, the penalty is a fine or imprisonment up to ten years or
both.

The United Kingdom law under the Computer Misuse Act 1990 provides for
1) Unauthorized access to computer mater program, or data U/S. 1 with a penalty of
imprisonment for 6 months and/or a fine.
2) Unauthorized access with criminal intent U/S. 2 with a term of five years and/or a
fine.
3) Unauthorized modification of computer material source code program or data U/S. 3
with a term of five years and/or a fine.

*Singapore law “The Computer Misuse Act 1998 provides for
1) Unauthorized access to computer material, program or data U/S. 3
With penalty of a fine up to $5000 or imprisonment up to 2 years or both.
2) Access with criminal intent U/S- 5 with a fine up to $50,000 and/or a term
up to 10 years.
3) Unauthorized modification of computer material, program or data
U/S- 5 with a fine up to $50,000 and/or a term of 3 years, but in case of any damage
caus e a fine up to $50,000 and/or a term up to 7 years.
The IT Act – in India provides the penalty U/S 66 (2) for hacking with
computer system with imprisonment up to 3 years and/or a fine up to two lakh rupees.
The Act U/S. 66 (1) defines hacking as an act 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 it’s value or utility or
affects it injuriously by any means. “The IT Act 2000 notified for implementation in
October 2000 explicitly deals with the following categories of cyber crimes only -
Tampering with a Computer Source Code.
- Hacking
- Publishing any information which is obscene
- Misrepresentation
- Publishing digital signature, which is false in certain particulars or for
fraudulent act.
It is obvious that it is silent on many types of cyber crimes. * 29

5.1.2 (b) – TAMPERING (SOURCE CODE)
All the digital databases and source codes are potential targets of hacking
and tampering by criminal intruders. One of the main purposes of hacking has
been to delete, alter or destroy source code and data resource of a computer. “The
single largest menace facing the world of computers, today, is the threat of
corruption and destruction of digital information induced by a human agent with
the help of various types of program. * 30

Causing defacement of interactive web sites has been a very common feature
in the cyber space. In all financial instruments, research centers and administrative
offices, the vital computer records are potential and rich targets of hackers.

And vital computer systems are compromised, controlled and used by
computer hackers in furtherance of the ill motive. The relevant laws on hacking as
a crime have been enacted by different countries.

29 * K K Bajaj ---------------Sup-21------------ P – 426
30 * N Kamath – -------Cyber Law ------ 2001-Universal Law Pub Co.-ND--------
- P – 283
The United States has framed laws on the possession, production and transferring of any access device (access tool) U/s. 1029, manufacturing intercepting-devices U/s. 2512; access any computer database with criminal intent U/s. 1030 (a) (5) A. The United Kingdom also has enacted criminal law. The computer Misuse Act - 1990 prohibiting:

1. Unauthorized access to computer material U/s. 1
2. Unauthorized access with criminal intent U/s. 3 (1) and U/s.3 (2) of the Act. To impair the operation of the computer of any program thereof. *Singapore under the Computer Misuse Act has prohibited-
   1) Unauthorized access to computer material program or data U/s. 3.
   2) Access to any program or data with criminal intent-U/s. 4

Unauthorized modification of computer material program or data U/s. 5 providing penalty of fine of $10,000 or imprisonment for three years or both and in case of second conviction, the penalty will of a fine upto $20,000 or imprisonment for 3 years or both. But in case of any damage caused the penalty will be a fine of $50,000 or imprisonment for 7 years or both. * The Information Technology Act-has provided for unauthorized access to computer material source code, program etc. and thereby a alter, add or modify or delete any program, source code etc. data therein U/S. 65 and also provides for a penalty of imprisonment upto three years and/or with a fine upto two lakh rupees.

5.2.1. (C) MALICIOUS CODE

These are commonly called computer virus, bug or worm Intact these are carefully and intelligently written realized only instructions in symbolic code. If the machine can't understand the instruction, it can't work. The computer program is written by programmers and is fed into the machine which then converts it into its' won machine language or binary code and follows the long chain of instructions step by step.

But the code writer, the programmer arranges the instructions on such a way that the machine becomes puzzled by tricky instructions and takes anomalous steps but does not stop working. This is called a malicious code or virus, worm or computer bug. "A computer virus is software program that can make copies of it...The virus looks for a place to copy itself from floppy disk to floppy disk or to a hard disk or to a writable CD-ROM or a tape. Some viruses work with e-mail....

*30 A

A worm also is a kind of virus and passes from one machine to other through communication line. A worm may enter the computer memory and continues to fill it with meaningless data or may continue sending messages to all e-mail addresses kept in the computer. Some anti virous software resources:--www.antivirous.com;www.av.ibm.com; www.virousbltn.com;

So far numerous malicious codes have been detected and some of them have caused serious damage to computer and the Internet. Some of these are:----- Morris Worm (1988), whale Virus (1990), Melissa Virus (1999), "I Love you" Virus (2000), Code Red Worm (2001), Nimda Worm (2001) etc.

Spamming is unsolicited e-mail messages huge in volume and number, mostly from unknown origin. The messages may be business related or otherwise but mostly fraudulent and unreliable. “Even if you don’t read the messages, you still use up valuable time-displaying the headers and sorting out and deleting junk mail....... Finally unsolicited commercial e-mail (UCE) costs bandwidth on the Internet that is, spam takes up computer processing power and other network resources that could be better used carrying legitimate Internet traffic.” *31 It may be like “Make money with your computer, work at opportunity” etc

Case: Cyber Promotions Inc. v America Online (Compu serve)

Cyber promotion a media company of Pennsylvania sent continuous stream of spam e-mail massages to AOL subscribers using AOL equipments and different ISPs. AOL urged ‘Cyber’ to stop flooding spam messages but without effect and then AOL made counter e-mail bombing on the ISP stations routing the cyber spam. AOL redirected the millions of cyber spam messages changing their header address to the ISP computers. And also blocked messages sent by “Cyber”. The Cyber Co. changed address code and used innocent sender address to evade AOL-scrutiny. And ‘cyber’ sued AOL in March – 1996 alleging violation of computer Fraud and Abuse Act 18 USE 1030 and other grounds. AOL also filed a complaint against ‘Cyber’ alleging false advertisement, false origin header, violation of CFFA etc. Held-AOL not violating 1st Amendment blocking the cyber-spam. An injunction was issued against Cyber Promotion Inc from sending spam mails. Judge James L. Graham observed that the continuous and huge e-mail using AOL equipment make a trespass to personal property as ‘use of personal property exceeding consent is trespass. **]

In another case –

ACLU-Pataki – 2001 (New York)

It was observed that the question of the state regulation on spam traffic passing through the forum state required legal response.

State of California, however enacted two laws (AB 1929 & 1976) In January 1999 to hold the spammers liable to the state jurisdiction and with a penalty of fine per spam message etc. To restrict spam-anti spamming software may be traced at :-

1) www.spammerslamer.com
2) http :// www.panix.com/e-spam.html

Anti spam software resource sites :-

1) http :// www.ca-probate.com/aol/junk.htm,

Complain against the spamming may be made to the spammer’s ISP or to

• Abuse@aol.com
• Abuse@netcom.com
• abuse@interamp.com

*31 sup—27 ------------------ 1997 -------------------p------ 176
5.2.1.e **DENIAL OF SERVICE (DOS) – ATTACK**

Denial of service attack is targeted to a particular server computer and a huge volume of e-mail message of the order of mega bite is sent to it, when the victim computer can't but receive it and thus remains engaged solely to receive it continuously for hours and days together. Obviously the e-launched a denial of service attack against ‘Panix-a New York Internet Service Provider, for nine days, nearly putting them out of business and severely hurting their customers in the process. The distinguished researcher William Cheswick agrees that DOS is significant challenge facing the security community. *32 The famous ISP America Online (ALO) often faces the problem of slowing down due to flood of e-mail garbage passing through it and consequently the customers are denied access to the Internet. There may be different types of DOS attacks such as Ping of Death, Trojan Horse, DNS service attacks, Fraggle and Smurf attacks.

The DOS attack broadly may be of two types saturating the carrying capacity of modern link line and crashing the target computer by pouring huge garbage e-mail message into the memory space. A DOS hacker can subscribe the victim to hundreds of news groups who will go on sending their messages to target e-mail message and the target computer will crash falling to process and accommodate such huge volume of e-mail message. A denial of service (DOS) attack is a type of network attack where the network bandwidth is saturated and legitimate users are denied services they are entitled to. DOS attacks are aimed at Web servers, application servers and communication links. Examples of DOS attacks are attempts to flood a Web server and a network with URL requests. DOS attacks can seriously impair the functioning of organizations, such as call centers, whose business depends on communication over the Internet.” *33 The causes of DOS attack may be found in the very nature of the Internet system and Internet application software. It is difficult to check this type of attack completely “Various reasons allow hackers to implement a DOS attack. Some of them are weakness of the overall system architecture, Bugs in the operating system or software loopholes in the system security.” *34

Some methods may be applied to check and reduce the DOS attacks such as the use of firewalls, by limiting network traffic.

Solving the problem of DOS is complex but it requires the assistance of all the Internet functionaries however when the communication line itself is filled up beyond capacity, inter communication among different servers computers becomes difficult. “Finding the perpetrators is even harder. The following diagram shows that in order to identify the bad guys, we have to be able to trace the connection all the way from the victim back to the source.” *35

Some of the information resources on the DOS attack –

- http://www.attrition.org/security/denial
- Attack tools – at
- Protection tools at
  - http://www.risecurity.net/security.com

The DOS may be treated as an illegal act of trespassing other’s computer.

32* sup – 20 ------------- 2000 -------------- 277
p--------229
34* sup --14--------2003------------------------p-----154
35* sup--20--------2k------------------------p--282
One boy from Pondichery conducted a DOS attack by e-mail bombing a target service provider in UK and then was traced by Indian Cyber police and arrested in ............ Mar 2002 and prosecuted U/S – 507, 509 IPC and also U/S – 66 IT Act.

5.2.1 F

**Porn Websites**

A very common problem in cyber space is the numerous porn websites and the exposure or access to these sites obviously caused serious injuries to the minors and young people. “The bottom line is that child pornography is illegal, penalties are stiff and it is politically correct to take a stance against it.”

In *American Civil Liberties Union Vs Reno* 1996 WLG 5464 EDPA. Reno placed pornographic materials on the websites and ACLU brought on action against it. The court allowed injunction in the case. In – *Shea V US* also the court granted preliminary injunction against the porn websites. However the right to speech and expression was sought to protect indecent, not obscene, communications as between adults. And it is really difficult to know the age of the user being below or above 18 years. *United States V Thomas – 74.F.3d.701 (6th Cir.1996).

The defendant ran a porn website and was closed by an order of injunction granted by the court under Federal obscenity laws. The court convicted the accused.

Case *Miller Vs California Vs L.ed. 2d. 429 (1973)*

The definition of obscenity was to be understood by what the average persons applying contemporary community standards would to be obscene. This standard has been known as the Miller Test of obscene materials.


The court framed the test for obscene materials on the basis of prevailing community standard.

The IT Act – provides the law U/S. 67 on publication transmission of obscene materials in the cyber space. The Acts provides for a penalty of five years imprisonment and a fine up to one lack rupees but for subsequent conviction the term may extend up to 10 years and a fine of two lack rupees.


- *United States V Dost-

The liability of the accused has been analyzed by the court and it was observed that the prosecution must prove the sexually explicit nature of the material in picture graphic or other visual form arousing sexual desire and also that the prosecution is required to prove that the persons depicted in the picture were minor (below 18 years of age).

- *Os borne V ohio – 495 US 103 Sct. 1691 (1990)*

In both the above cases, the court observed that the state under compulsion to protect children, can treat and declare child pornography a contraband.

- *United States - V - Knox 977 F.2d.815 (3rd cir.1992)*

The court held that in order to constitute a child pornography the child does not need to be nude-but the focus on the private parts of the minor females would be sufficient to constitute child pornography.

To protect the children from porn websites ‘filters’ may be used and the necessary guidance may be had from some relevant sites. Net nanny, surf watch and cyber sitter provide automatic filters which block undesirable sites. Cyber snoop software may be used to track and record all activities in a tamper proof file in the computer to know the movements of the child concerned. The site www.cyberangel.org/safety and privacy/chart html also provides filter programs.

Some resources for protection and guidance-
- www.safekids.com
- www.cdt.org
- www.cyberangel.org

5.2.1. g - CYBER FRAUD (SCAMS)
Cyber space being the mirror of the real space all traditional crimes also appear here. So the fraudulent activities also are very common in cyber space whose various advertisements and invitations appearing innocent may defraud netizens. “Internet fraud is a form of white collar crime whose growth may be as rapid and diverse as the growth of the Internet itself. According to the consumer organization, Internet Fraud Watch, the number of consumer complaints it receives about Internet fraud schemes, has risen dramatically in the past two years from 1152 in 1997 to more than 7500 in 1998”* 37

There may be various types of cyber fraud like Online Investment, Online Auction, or Make Money with your computer etc.

Some important points to spot the Internet scam
1) If the person concerned requires cash payment and avoids online payment.
2) Check the e-mail address to be genuine one if not look for a physical address, real phone number and to contact a human.
3) Always use a credit card for payments.
4) Transactions should be made with known companies only.
5) Not to provide unnecessary personal information to the other side.

Fraud report sites –
1) Internet Fraud watch – www.fraud.org. Or 800.876.7060
2) Fax to S. Florida Task Force – 954,925,1362
3) www.fraud.org
4) www.locus.haleyon.com

US Code provides for cyber fraud under section 1030 of Title-18
The Indian Penal Code- 1860- defines fraud U/S. 25 as an intentional act to deprive a man of his right to some property ,opportunity or comfort.

5.2.1.h. MISCELLANEOUS CYBER OFFENCES
Cyber stalking is online harassment of the citizens. It may take various forms ranging from sending false information as to some subject of personal information or false advertisement of posting in cyberspace about any individual like e-mail - ‘you are in terrible danger’, ‘beware yours kins are now in danger’, etc. The nature of stalking may be related to sexual harassment, love obsession, hate and revenge attitude etc. “Cyber stalking refers to the activity of users sending harassing or threatening e-mail to other users. 19 * 38
The telephone hackers (phreaks) of 1960s 1970s quickly developed themselves to computer hackers, 2nd generation hackers in 1970s and 1980s. And they again improved their skill in 1990s onwards to hack Internet resources (3rd generation, we may say). Now the hackers' own websites provide tools (software) and techniques some of these are www. anonymizer.Com; http://www.replay.com/remailer; http://new order.box.sk; http://www.2600.Com; etc.

The Various steps of hacking may be as below :-

(A) * Just like the bank robber in a mask, criminal hacking needs additional layers of anonymity to stay off the Police radar screens.

* With hacking, though anonymity is often achieved by creating new 'people'.

(B) * ROOT-ACCESS:

Hackers first acquire control of portion of weak networks like universities, academic institutions—lax in security practices—for open and free exchange of information— or like.

Contd...P/2..
WEAKNESSES

These other websites—due to fairly simple logon processes and weaknesses—are selected as platforms.

(C) * Once a hacker has found his way into a system from his real a/c. or from a free aOL a/c. his first task is to set himself up as a new user.

With root access, the hacker sets up a new user with any name, he chooses and a password.

(D) * when he is satisfied he is anonymous enough, he will attack his target.

* The reason for his multiple hops is to make law enfor-
cements job really tough.

* Hacker can install a small program to erase his tracks.

* Spoofing—is a cheat—deception or lie a way of anonymizing—using e-mail with false address as sender.

Hackers sites Contain large no. of password cracking programs for almost any imaginable operating systems:

Contd.P/3.
- SNIFTER -

* All they need is a Computer with a common network card and some sniffer software.

The network card has to be put (into promiscuous mode)... the Computer will then listen to all network traffic that is sent back and forth.

all of the traffic that travels up and down a network is Captured at a single Computer. The messages are captured and then can be stored in a file for later analysis.

So the hacker can learn- many things :-

using the sniffer :-

1) Users names and passwords for use at a later time.

2) High level dialogues (e-mail and attachment)between senior executives on sensitive corporate matters:

   finance, sales, ......

3) Highly proprietary inform.../...-

(F) TROJAN SNIFFER : is a sniffing program, generally small, is secretly installed into a network server, or a Computer
of interest, if done well, the program is hidden from the view of the network administrator.

* Silently, the sniffer will collect the traffic on that computer and either store it in a secret location for later retrieval by the hacker or in some cases, send the gathered network traffic to a distant computer.

* Finding a sniffer on a network is tough, since then operation is virtually invisible.

(G) Next step to hacking:

Penetration testing:

1) Assess the strength and weaknesses of the network.
2) Determine the Vulnerabilities in the system.

Then collect: Open source informations:

1) operating systems.
2) Open technical systems in use.

F.O.R.:

* Network information:

www. cyber army, com - gives information of target network if IP address is put into it.
* Another: 'Netlab' - a freeware - from 
www.eb.uah.edu/N adani1/ for basic analysis.

The attacker wants to know as much as he can about a target.

(H) SATAN - a tool used by system administrators for
Analyzing networks-it recognizes-several Common network
related security problems and offers an explanation and
impact, also provides solution like-correct an error,
install a bugfix, restrict access...or disable service.

New Vulnerabilities pop up every week.

SATAN like tool you where the electronic doors are ajar,
where windows are cracked where there is no perimeter-security
at all.

(I) FINAL ACT - Breaking in -

Based upon the findings from Scanners, social engineering,
open source intelligence-access is gained through multiple-
entrances-maintenance ports-FAX to data lines dedicated net-
work-telephone networks - etc.

Next step is to employ technical means-tools are used to break
passwords-etc., to employ programs-to by-pass security
systems-use own tools or find from the Internet also through
telephone and FAX system.

***
5.2.2 CYBER OFFENCES AGAINST INTELLECTUAL PROPERTY

Intellectual property is a product of human intellect that has commercial value – wide range of creations like artistic & literary works – fiction songs, poetry – design or product – name, mechanical engineering invention, chemical formula, machines, computer hardware and software etc. IP right as a property can be bought, sold and licensed and naturally requires to be protected in favour of the owner of the I.P. The name industrial property is also used to indicate. Intellectual property with the advent of cyber space through the Internet the I.P. has been in important issue for law. The cyber space has created new challenges for law enforcement authorities in various fronts including this I.P. right.

CASE: UMG Recording – VS – MP3.com – 92f.supp.2d.349

The Internet being a global phenomenon various attempts are made at the International level. International bodies are not new thing in this 29th Century like GATT, WTO, UN etc. “The GATT provisions were revised in 1986 to include Intellectual property as a subject of International understanding. The most important part of I.P.L violation in cyber space is in the copy right law and Trade Mark Law. The Internet is operating as a vast copying machine active through the globe beyond the reach of any legal system whatsoever. So the right to copy and reproduce has been jeopardized to a great extent. “For more than a century, our system for protecting intellectual property rights has fostered the creativity of artists and inventors. But now it is being challenged by two major global forces: the Internet which can act as a gigantic international copying machine and a global health crisis in which patented miracles drugs are expensive for developing countries.” *40

It is observed by some legal experts like Bruce Lehman US Commissioner for patents and Trade marks (1993-98) that the system is not broken and the existing law can with stand the new pressure, Previous Technological challenges like fax machines, VCR have been successfully overcome. But some other experts like Lester C. Thrown an MIT economist observed that a new legal system require to be developed to face the recent technological challenges. However it is clear to all concerned that 21st century framework for IPR needs to make a balance between the conflicting interests of the artists and inventors on the one hand and the interest of the users And the public on the other.


One such critical issue arose on the price and distribution of patented AIDS medicines in Africa. The pharmaceutical companies are in confusion. When Merek & Co. slashed its prices for those particular vaccines and relaxed the patent rights just for South Africa for humanitarian grounds where 15% of adults are carrying HIV virus, the manufacturing companies filed lawsuit preventing South Africa from locally producing or importing cheap generic items. It appears that the existing legal system (statutes, values and jurisprudence) is at a cross road to meet the challenges posted by cyber space or borderless civilization of 21st century. Recent technologies MP3 and Napster have created serious challenges to the copyright law.

The MP3 stands for Moving Pictures Expert Groups (MPEG) 1 Audio Layer – 3. It is an encoding technology to compress a digital music file by a ratio of 12:1. “As the usage of the MP3 technology allows not only the ability to download music from the Internet in the MP3 format but also the distribution of MP3 audio files over the Internet, special software called ‘ripper’ has been developed. Which allows the conversion, ripping of music from CDs to MP3 audio files. The ‘ripper’ is available on different Internet sites for free – http://www.nytimes.com/library/tech/99/07/biztech/articles/18mp3starauss.html.” *41 Also http://www.napster.com or www.mp3.com

41* Article & Web alert – Jan V Feb 2002 AIRC US Embassy American Centre – New
5.3 CRIMINAL LIABILITIES IN CYBER SPACE

The issue of criminal liability of various cyber activities like hacking, malicious code, porn websites uploading and downloading of materials, cryptography, framing spoofing etc. have become a question of endless debate. Especially the debate goes on between Criminal Lawyers, jurist and advocates of civil liberty and human rights on the one hand the law Enforcement Agencies (LEAs), social workers and the governments on the other hand. The rules of liability applied in real world, however find some difficulties in the virtual space on the question of physical access remote acts, communication lines connecting on-line computers etc. "We must understand that the virtual presence of the hacker is never enough to constitute a crime what is always needed is a body, a real body, a live body, through which law can institute its' well established exercise of power."

On the basis of the cause and effect relation, different undesirable activities in the virtual space have been subjected to criminal law. The traditional rules of criminal act have been applied as far as possible.

Meli and others V R (1954) All ER 373 where the accused (appellant) assaulted the victim and rolled the body over a cliff and the victim was dead. Through the medical evidence established that the death was caused by exposure to cold not due to assault or fall

In R V Khandu – 1890 – ILR Bom 1994 The accused assaulted the victim in side a hut and then set it on fire to remove all evidence Medical Evidence confirmed death by fire not by assault.

In R V Chiswibo 1961 The accused hit the victim on his head and put him in a hole and thus caused death – held guilty of attempted murder. In cyber space the link between the actor and the effect may be very remote and confusing but the liability can’t be denied.

As in case –

United States V Thomas – 6th Cir. 1996

The defendant operated a pornographic bulletin board from their home California. The BBS provided about 14000 Graphic files for members having password. But once from Temp. hit upon the contents and complained of obscene materials held liable and convicted applies rule of personal jurisdiction.

Again in the case –

United States V Czubinski – 106 F.3d.1069 1st Cir. 1997 Richard Czubinski an employee of Taxpayer Services Department at Boston – used to access and view numerous files of different taxpayers computer using password and access code. Forensic audit confirmed his unauthorized accesses. He was convicted U/S. 1030 (a) (4) for computer fraud through he did not disclose or sell such information. On appeal the Supreme Court reversed the Judgment as he took access and took nothing of value. And as such – had no criminal intent.

5.3.1. PRESENT LAW OF CRIMINAL LIABILITY AND THE CYBER CRIMES

The rule of strict liability of the 15th Century was refined by the rule of mens rea in 18th century in the case : Fowler V Padget (1798) 7 TR 509 TAC

Chief justice Kenyon in 1798 “The intent and the act must both conquer to constitute the crime” *43

---

42* sup – 4 -------2000 ---------- P-21(2)
And thus the rule: 'actus facit reum nisi mens sit rea'—was established which required the actus reus—(active conduct) and mens rea—(guilty mind) for the purposes. But injury caused to a patient by doctor/surgeon invites no criminal liability due to consent of the law and the consent of the patient.

Case: R -V- Van Butchell(1829) 3C and P 629
But there after in 20th century this rule of 'mens rea'(mental element) has been excluded in many social and economic legislations. But this new position has been revised and the present rule is that unless any legal provision expressly excludes the need of mens rea the element must be applied to impose criminal liability on any act in the case of statutory offences. case: - R - V -Prince (1875) 2 C C R. 154 T.A.C. accused was convicted of taking a girl assuming that she was over the age of 16 years. But in Kay - V -Butter Worth (1945) SJ 381. The driver was exempted from liability under Road Traffic Act as he was over powered by drowsiness. Or R -V- Tolson (1889) 23 WRD 168 where second marriage was excused for honest belief of the death of the spouse before 7 years elapsed. The rule of liability at present provides that the conduct must relate to 'actus reus', voluntary and the actor having knowledge of consequences. But the liability can be varied due to mistake, compulsion and necessity etc. In cyber space the element of 'actus reus' and mens rea—are not always available and physically linked. "the second paradigm- criminal intent is under fire in the realm of Internet prosecution ... In many cases hackers gain entry just for the fun of it." *44

United states -V- Czubinski-106 F 3d 1069 (1st Cir 1997) where the defendant employee accessed numerous taxpayers files kept in the employer company's database. Held liable for unauthorized access and fraud under USC 1030 (a) 4. but on appeal convicting case quashed as the defendant had no equality mind except viewing the tax files of known persons. So, exempted from liability due to the absence of quality mind.

In US P. Mass. 1994 The defendant collected and uploaded popular software's and computer games and made available to pass word holding members through a bulletin board: He was charged with the violation wire fraud statute. but court realized him as he did not receive any financial gain. Case:- Yahoo Inc.- V- Akash Arora & Anr.The defendant setup a website Yahoo India. Com where as the famous media company yahoo Inc. (registered in 1995) and this caused confusion in cyber space. The defendant continent that (1) lain tiff trade mark not registered in India (2) the defendants are not offering any goods or services to attract junction of passing off, (3) yahoo is a general dictionary word. Whence has no distinctiveness (4)the defendants used a disclaimer. But the court rejected all the places setup by the defendant and granted interim injunction in spite of the distinctive word "India" added with Yahoo. Again Personal Jurisdiction was allowed in ACLUV Reno 1996 against the website on child pornography and also in the case USV Thomas-1996 against pornographic content in the website but denied in - Preskap -V- System One (1994) and in Mc. Donough -V- Fallon (1996) simply on the ground that the websites are accessible from other states. Other case :- Jews for Jesus -Vs- Bordsky- 46 US Pq. 2d 1652.

5.3.2 DIFFERENT NATIONALS LAWS
THE criminal liability for hacking and other cyber wrongs have been established in different national legislations- (A) the United States of America

(1) THE Federal Criminal Code related to computer crime (Title- 18 Part I chapter -47 provides for criminal liability U/S . 1029 for production or use or trafficking counterfeit, unauthorized access devise and also U/S . 1030 for taking access to and obtaining information protected against disclosure for various antinational and illegal activities. The provision U/S .1029 thus criminalize the possession of illegal access device s and S/1030 criminalizes the unauthorized access to officially protected information vital to national security or commerce. Cyber crime legislation has been adopted at both the State and Federal levels—section-1030 of Title 18 of the US Code defines a number of computer related offenses e.g.hacking ,cracking,virus dissemination, password-trafficking,extortion and fraud."*45
The United Kingdom

173

The UK enacted the Computer Misuse Act – 1990 to make provisions for securing computer material against unauthorized access or modification and for connected purposes. The Act penalizes the following acts –

- Access to Computer Materials—The Act imposes criminal liability for accessing a computer material U/s − 1, with or without any intent to reach any particular data a with a penalty of imprisonment for six months or fine or both.

1- Hacking — Access with guilty intention : - A person taking access with intent to commit or facilitate commission of further offences will be sentenced for six months or fine or both (section – 2)

2- Cracking : -- Modification or Tampering with computer material – U/s – 3 A person is held liable for causing modification of any computer material, the intent may not be directed to any particular data, content but with intent.

(a) To impair the operation of any computer
(b) To prevent access to any program/data.
(c) To impair the operation of any such program.

But the intent may not be directed at any particular computer, program or data. The offence U/s. 3 attracts a penalty of 6 months imprisonment or fine or both for summary conviction but for graver offence it extends to 5 years or fine or both.

3- Fraud : any access with guilty intent to commit further offences – is criminal wrong u/s – 2.

4) Malicious code – to impair the operation of any computer, U/s. 3 (2)a

5) Any act – to prevent or hinder access to any program or data held in any computer U/s – 3 (2) b.

The Act also provides for law of jurisdiction- U/4,5,6,7,8 and 9. The law u/s. 5 proceeds for criminal liability to the accused if he is in the home country at the time of commission of the accused takes unauthorized access to any computer kept in the home country.

It is observed that “The Act creates three distinct offences : unauthorized access to computer material unauthorized access with intent to commit or facilitate commission of further offences, and unauthorized modification of computer material—one criticism levelled at the Computer Misuse Act is that it needs to be revised. since it ‘takes not account of the Internet, and has not yet been updated to cover offences such as denial of service (DOS) attacks. * 46

( C ) ---- In Australia – The Cyber Crime Act – 2001 deals with different cyber crimes under division – 477 – serious computer offences. The Act imposes criminal liability in the following fact situations.

Access – Every unauthorized access to data, data modification, impairment of electronic communication to or from a computer, access in connection with some other crime, or access through telecommunication service liable to a penalty of life imprisonment or 5 years U/s. 477-1

Hacking:--- Unauthorized modification of data to cause impairment, attracts absolute liability with – a penalty of 10 years imprisonment U/s – 477.2 liability is made out for modification only irrespective of impairment.

Network --- Dislocation/Disruption – attracts 10 years imprisonment U/s – 477.3.

46 * Sup – 8 ---- vol – 1 -----------------------2005--------P---193
(D) In Singapore ---- The Computer Misuse Act – 1993 - provides for criminal liability in various cyber wrongs.

Access- Any unauthorized access to computer material attract a penalty of fine or imprisonment for 2 years or both u/s. 3.
Hacking----- access with criminal intent is liable to be punished by a fine or imprisonment for 10 years or both u/s-4.
Modification or tampering with data----- attracts a penalty of fine or imprisonment for three years or both U/S-5.
Interruption or use of computer service----- is a criminal wrong to be punished with fine or 3 years term or both U/s-6.
Obstruction ------is to use of computer has been a wrong punishable with fine or 3 years imprisonment or both U/S.7.
Discloser or access code or password----- attracts a penalty of fine or 3 years imprisonment or both u/s-8.

The Act provides for more stringent provisions in case of wrongs committed to computers related to the National Security, Legal System, Communication and essential services and provides for penalty of fine ($1 Lac) or imprisonment for 20 years or both U/s – 9. The Act also provides for the same liability in case of abetment and attempt irrespective of the actual commission of the intended offence.

E) In Malaysia --- the Computer Crimes Act 1997 also provides criminal liability for similar cyber wrongs – The Act penalizes (1) the act of unauthorized access u/s-3 with fine and/or imprisonment for three years. (2) the act of fraud etc. through the computer U/s – 4 with a penalty of fine or term of 10 years a (43) the act of communicating access code-program, password to others u/s – 6 with a fine and/or a term of 3 years (5) the act of abetment or attempt to commit any above mentioned crime U/s-7 with a fine and/or a term equal to the offence concern that in case of any act of preparation or act in furtherance of the offence – the penalty will be one half of the penalty provided for the offence in question (6) the act of illegal possession or control of any program data or information u/s-8 with the penalty of taking unauthorized access to the same data or information.

(F) INDIA

The system of liability under the Information Technology Act has been divided into two broad divisions – on under civil management and the other under the criminal law. The IT Act provides criminal liability to certain acts and omission described under Chapter – XI (SS- 65 through 75). The Act here provided for specific Internet crimes under the title Hacking U/s-66 and Tampering with computer source documents u/s 65 and publishing obscene materials u/s 67 of Act. “The Indian Act was mainly based on the UNCITRAL Model Law on Electronic Commerce----- Since the Indian Act is based on this Model Law, it can be seen that its focus is mainly on regularizing e-commerce. It does not focus its attention towards combating Cyber Crime as such. However it contains certain provisions that deal with offences falling under this genus. “

The cyber wrongs otherwise known as crimes in different countries such as malicious code, unauthorized access and download of data, damaging computer system, blocking access etc. have been kept outside the scope of criminal law.

5.3.3. CONVENTIONS & RECOMMENDATIONS ON CRIMINAL POLICY (CYBER CRIME)

The Organization for Economic Co-operation and Development (OECD) took initiative in early 1980s to develop a policy on cyber crimes. And in 1986 the OECD prepared a report on – Computer Related Crime: Analysis of Legal Policy. The OECD report defined the offensive act as

(1) Any addition, alteration, erasure of Computer data/program with a criminal intent to transfer fund or anything of value.
(2) Any such act of input, alteration, erasure of data/program with intent to commit forgery.
(3) Any such act to hinder computer functioning or tele-communication system.
(4) To exploit and to market any computer program without consent of the owner.
(5) Any act of unauthorized access or interception of a computer or telecommunication system.

In 1989 Council of Europe- Select Committee of Experts on Computer related crime adopted a set of Recommendations. This report provided for a minimum list of cyber crimes containing unauthorized access, and interception, computer fraud and forgery, damage to data or program, computer sabotage, unauthorized reproduction, distribution of a computer program and some others on the optional list as alteration of computer data/program, unauthorized use of computer or program, computer espionage etc.

In 1995 the UN published a Manual on the Prevention and Control of Computer Related Crime.

In 1995 the Interpol also held 1st International Conference on Computer crime the other conferences were held in 1996,1998, and 2000,2002 (Seoul).

In 2001 the Council of Europe Convention was held in Budapest. The convention provides for criminal liability in different cyber wrongs such as —

Article-2---- provides for illegal access to computer system.
A/3 – unauthorized interception by technical means, A/4.--- any damage, deletion alteration of data, A/5 -- any act of hindering – the functioning of computer system by damaging or altering the computer data – A/6---- production, sale or procurement of access device, program ,password, code etc. A/7 - Any act of forgery involving computer/computer system.A/8 - Fraud involving the computer.A/9 - Child pornography and related offences.A/10 -- Copyright infringement and related acts.
A/11 -- Liability in case of attempt and aiding or abetting.
A/12 – Provides for corporate liability in cyber offences.
A/13 – Provides for effective proportionate and dissuasive sanctions including deprivation of liberty to both natural and legal persons concerned.

The Convention drafters' principal concerns were two fold. First they wanted to ensure crime definitions were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve. Second the drafters wanted the Convention to remain sensitive to the legal regimes of domestic states. ”*48

The UN Information Security Permanent Monitoring Panel (PMP) estd. in 2001 also prepared a set of Recommendations.
5.4.1 - ROLE OF ISP IN CYBER SPACE

The Internet Access Providers actually technical counterparts of the Internet back bone lines and operate as transit points for Internet communications. The end user riches first the ISP and then the Internet. “An ISP is a company that provides access to the Internet. usually through local telephone lines. Examples of ISPs include AOL, Prodigy, Yahoo and Compu-serve. ISP liability is the issue of whether an ISP can be held liable for the products and services it provides, the way in which it does business and / or the tools that it uses to conduct that business. * 51

Thus the ISP serves as the gateway for all the data traffic coming to and from its subscribers for which he can’t have control or liability generally. But since the data traffic pass through the ISP-processing computer, the ISP concerned has an opportunity to intercept or monitor the data, check or block some kind of data traffic using filters or other devices. “On the Internet, for example, an Internet Service Provider can watch almost everywhere we go, and can record with whom we communicate. At the same time and on the other side of the issue, anonymous Web browsing service permit maintaining privacy regarding our web browsing habits, anonymous remailers provide untraceable and anonymous communication and encryption can provide complete confidentiality of content. Technology in other words, can provide either no privacy or perfect privacy, sophisticated users can have near privacy, where common citizens have little unless they are aware of the consequences of their actions and act accordingly”. * 52

Thus gradually with the spread of criminal activities like hacking, worm spreading, DOS, spam etc. the law enforcement agencies looked for help from the ISP – units. And in many cases, the concerned ISPs were involved in criminal litigations. In case of spam e-mails both the Service Provider and its’ subscribers suffer. In 1996 AOL, the service provider blocked millions of spam e-mails passing through it, directed to its own subscribers and AOL redirected the same to the origin Cyber Promotions Inc. – another ISP. The Cyber Inc. then sued AOL but the court held AOL not liable for violation of Computer Fraud Act U/s. 1030 and 1st Amendment Right. Case : Cyber Promotions Inc. V AOL – 1996 And an order of injunction was issued against the Cyber Co. not to allow spam e-mails to pass through its network. California passed two laws on spam e-mails under the Act AB 1629 and 1976. The spam Law. Provided for damages of $50 per spam massage to be recovered from the spammer.
Case : Lunney V Prodigy, 94 NY. 2d 242 (1999)
The plaintiff was victim of harassment due to the fact that some offensive materials were sent to some third person using plaintiff’s name as the sender. The offender, a prankster had opened an user account with the ISP prody. Who was alleged to be liable to open such an account in false name and also to allow offensive materials to pass through its network.

NY Court – held that ISP can’t be made liable for the content of e-mail messages sent or posted on their networks. The Supreme Court also upheld the same view holding the “compelling an ISP to examine and screen millions of e-mail communications...and to require an ISP to screen all potential customers and transmissions would subject them to an unreasonable amount of liability. * 53

51*Sup-36 -------------- 2001 ------------------------P- 1056
52*Sup-4 ------------- 2000 --------------------------P- 141
53* Sup -36---------------2001 ------------------------P- 1056
Case: Specht - V - Netscape and AOL. - NY. 2000

The complainant alleged that Netscape and AOL continuing surveillance and spying on his internet activities using Smart Download given to their users. And whenever any user downloads any Zip or exe file a copy of it is transferred to the defendant's site (with the help of cookies installed in the users computers) and thus developed a detailed profile of the files (ZIP file is a compressed file format. To uncompress PK Zip (DOS) or Win Zip (Window) are required. And exe file is a self extracting file that decompresses when loaded. No separate utility is needed to decompress it). The complainant claimed damages for the theft of the private information U/S 2511 and S/2520 of Electronic Communications Privacy Act and U/S. 1030 of the Computer Fraud and Abuse Act.

In the mean time, an expert group (P8) on Misuse of International Data Networks appointed by G 7 countries, Russia and European Union presented a report in December 1997. This expert group urged members to make rules assigning the ISPs the reasonable duty to erase illegal contents and assure free data flow.

The Internet Industry Code of Practice framed in May 2002 by Internet Industry Association (IIA) (www.iia.net) also provides for ISP obligations in relation to Internet Access generally U/S. 5 and 6 of the code. The Cyber Crime Code of Practice made in July 2003 by IIA provides for ISP obligation to assist the Law Enforcement Agencies (LEA) U/S. 1.4, 1.5 : 1.6 and 1.6 of the Code.

Germany has passed a law making ISP responsible for the content on their system on the plain reasoning that what is wrong off-line will be equally wrong on-line also. The Singapore Electronic Transactions Act- 1998 also provides for ISP liability U/S. 10 of the Act. In a case: Play boy Enterprise - V - Frena - F. Supp. 1993. Digitised images of playboy were placed in bulletin board by some 3rd party but in action of copy right infringement, court held the media (bulletin board) liable. New York Times - Vs - Sullivan - 376 US (1964) The New York Times was held liable for publishing an defamatory advertisement. But on appeal the Supreme Court reversed the Judgment and observed that intermediaries cant be held liable to make them afraid to publish. Again - Cubby Vs Compuserve It was observed that Compu Serve an ISP - media company can't be held liable for a defamatory message posted in its conferences. The court held that constitutional guarantees of Freedom of Speech and Expression stands on the way of imposing strict liability here. In this observations, as a whole liability can't be imposed on ISP for any criminal message passing through it.

The Information :chnology Act deals with the role of ISP U/S. 79 of the Act. The Act provides Network Service Providers not be liable in certain cases for the removal of doubts. It is hereby declared that no person providing any service as a network provider, shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation - For the purposes of this section –
(a) 'network service providers' means an intermediary.
(b) 'Third party information' means any information dealt with by a network service provider in his capacity as an intermediary. But in view of increasing criminal activities in the cyber space, the active assistance of the ISP servers are very much valuable to the LEAs. And hence not only filtering and blocking the undesirable and harmful traffic but to track and trace the network offenders the active role of the ISPs are real need of the hour. The conceivable purpose for imposing criminal liability on the intermediaries is to change their behaviour discourage them from handling material that might turn out to violate the criminal law. * 54

54 * Sup – 36 ---------------2001------------------------P--562
At every crossroad of human civilization, the human society being led by its soul and conscience has responded to and stood against all inhuman activities, systems, rules, oppression and all forms of domination coming mainly from superior corrupt social economic and political powers. The human rights thus mainly relate to a set of rights very fundamental and vital to the very existence of human being, complete development of health and mind of an individual. The Natural Law in Europe in 15th 16th century stood for these rights.

Thomas Hobbes (1588-1679) in UK and John Locke (1632-1704) advocated for the same set of rights in new name the Natural Rights. “The individual retained the natural rights to life liberty and estate for they were the natural and inalienable rights of man ..., The purpose of government was to protect these, it has no other end than ‘to preserve the members of that society in their lives, liberties and possessions. As Locke put it all this is limited to the public good of the society. so long as government fulfills this purpose, its laws should be binding. When it ceases to protect or begins to encroach on these ‘natural rights’ laws lose their validity and the government may be overthrown”55 The validity of Law, justification of government action thus stand the test of natural rights which advocate for the self preservation continuity and perfection of man.

The issue again came up with the massive oppression destruction and killings of citizens by political governments in different countries during 1st and 2nd world war. Then the human conscience stood for the protection of individuals and drafted a detailed set of rights under the Universal Declaration of Human Rights in 1948 which stands as a standard to all human societies. The other documents like International Covenant for Protection of Civil and Political Rights (ICPR) and Social and Economic Rights (ICESC) were made in 1966 and some other instruments also came to be recognized. And the Right to life and personal liberty U/A-3 of UDHR A/6 of ICPR. The Right to Privacy U/A -12 of UDHR; A/17-ICPR,And the Right to speech & expression U/A -19 of UDHR; A/19-ICPR And the Right to property U/A-17 of UDHR;

In India the National Government has rightly accommodated the natural right or human rights under the part III. Fundamental Rights U/A 14 -30 which provide for equality(A/14), nondiscrimination (15,16,17), six basic freedoms like speech and expression, peaceful association, movement, resident (livelihood U/A-19 etc. Right to life and personal liberty U/A-21 and some other.

In cyber space or virtual world the intrusion and damage caused by hacker among such other wrongs has been serious concern to privacy, security and property right on the one hand but on the other hand the law enforcement agencies are becoming over aggressive to encroach the freedom of speech expression and communication among the people. The question of intrusion, interception and surveillance has been equally injurious to the people.

However main issues in the cyberspace as to Human Rights have been privacy, freedom of speech and expression, right to property and right to communicate with others beyond national border. "There are many private activities that are being carried out through the medium of Internet. Merely because it is being carried out in the Internet does it lose its private character? For examples, what happens to the fundamental human rights like freedom of expression, freedom of association, freedom of political participation, freedom to privacy? Can the Government stifle these freedoms in the guise of regulating Internet? These are very important question that affect the human rights of the netizens."*56

(b) HUMAN RIGHTS ISSUES IN CYBER SPACE

Some of the burning questions in cyber space in this subject are privacy, freedom of speech and expression, communication and right to property.

Privacy- The issue on the right to privacy has become very complicated due to the fact that ill motivated persons are taking full advantage of this opportunity through natural anonymity in the Internet, application of cryptography, using devices like anonymous remailer etc. The illegal intrusion, interception surveillance, hackers also create a threat to privacy of data resources in the cyberspace.

United States

V

Czubinski.- 106 F.3d 1069 1st 1997)

Richard Czubinski, an employee of a Boston Taxpayers’ Services Division, access files of numerous known and unknown customers, friends, acquaintances and political rivals. Forensic audit trails established his illegal access exceeding his authorization. And held liable U.S.1030 of US code and convicted. On appeal however he was exempted from liability on the plea that he got nothing of value and he did not record or divulge the information to others except to satisfy idle curiosity. On judicial scrutiny of private content using personal pass phrase – People – Vs – Price. *56A

The other side of the threat to privacy of course comes from the LEA and state laws. The interception laws (USA,UK) search and seizure and confiscation in many cases are excessive. One Steve Jackson, owner of a computer game company, was arrested in 1990(March) and the US secret service, with a search warrant, confiscated computer hardware and software business records almost everything they found therein. “Steve Jackson owner of a computer game company lost his business to over-aggressive FBI agents when they suspected one of his employees of “cracking “ breaking into other peoples computers”. *57

56* sup 49---------2004 -------p-242
56A * sup – 4 ---- 2000 ----- p ---116
57* sup -3 -----1996----------Foreword(xii)
In another case, the excessive harassment invited civil action for damages. Case: United States v Hunter 19 F. Supp 2d 574 (D. VT. 1998). The US government conducted a search of attorney's home with a warrant to seize all computers, storage devices, software systems. It did not limit the search to the home office or make any list of specific crimes for which the search was allowed. The court thereafter agreed with the defendant that his 4th amendment right had been violated. The search and seizure also should be conducted under the dictates of rules of law not to be capricious and unlimited in scope. Because it is observed that "Information is valuable but privacy is priceless."*58 It is also seen that "privacy is at the soul of being human".*59 Case: Katz - Vs - US. 389 US 347, 362 (1967) - Reasonable Expectation of privacy. So the policy is that crime is to be detected, pursued, traced, and prosecuted but protection of privacy is to be upheld. "Even with a good framework of laws and codes of conduct, we need an effective way to deal with those who violate them. It follows, then that we would want workable agreements between physical governments so that criminal activity can be investigated and prosecuted without sacrificing our privacy (or other) rights."*60 Expression: the scope of speech and expression has reached a revolutionary stage when any human being can connect with any other at any place in real time with almost no cost. The telecommunication system is completely under commercial control as against the Internet. But many political governments are in a position to impose border on the information high way. "In recent crackdown on dissent in Viet Nam, at least 10 individuals have been arrested for exchanging e-mails with contacts in the Vietnamese Diaspora, posting articles critical of the government on the Internet and expressing dissenting opinion."*61 The other side of the freedom of expression is the illegal or porn. contents. Many legislative and judicial attempts have so far been made to manage this issue over cyber space but has remained unsolved. The confusion between indecent and obscene material remains as to the prevailing community standard.

Case: (1) Miller v California-1973 (2) US v Thomas -1996 (3) Bern Stein - Vs - US (1995) - Encryption program web site. The problem is based on the issue that how far the cyber space requires to be protected whether like a defense department or like a hospital or residential area or simple community centre having all elements of the real space. "What we should aim for is to achieve a fine balance between the rights of the society at large, similar to that of the real world criminal law."*62

58* sup-27 ----1997-------- p-28
59* sup-4--------2000-------- p-193
60* sup -3--------1996---- p-172
61* sup 47--------2004-------p-243
62* sup 49 ---------2004------p-249
Legal control is the most effective means to control crime in society. Because criminal science, of which criminal law is a part, deals with the study of the criminals' causes of crime (criminology), the study of effective measures to reduce the volume of crime in society (criminal policy) and the study of criminal legislations (criminal law). As a part of social science criminal law thus relates to the scientific control and management of undesirable activities. Also that the legal control is effective in the sense that it emirates from the government policy and takes the help of a very powerful infrastructure of the legislature judiciary, police and prison system. And the prevailing legal system along with rules and principles can deal with the problem of cyber crime subject to some modifications and new additions of rules and principles rather refinement of legal concepts. “Since we already have a great many laws on the books lets use them. Most of those laws apply to cyber space, a whole new set of laws just for the Internet is neither necessary nor desirable”. * 63

The legal control of cyber crime as usual relates to the traditional form and steps like. Detection Recording Reporting Complaining to LEA Investigation Track and Trace, Interception. Prosecution – Trial – Search & Seizure Evidence Judgment conviction or acquittal (prison – probation). But every minute step starting from detection to the end conviction acquittal or imprisonment is a part of legal control taking law as technology. The Realist Jurist Karl N. Llewellyn (1893 – 1962) observed “This doing of some thing about disputes, this doing of it reasonably, is the business of law And the people who have the doing in charge, whether they be judges, or sheriffs or clerks or jailors or lawyers : are officials of the law what these officials do about disputes is, to my mind, the law itself”. * 64 In cyber space all the basic principles of law apply equally as in real space as because the nature and scope of human rights prevailing social values and norms are relevant also for citizens who are in fact real and natural persons.

The legal control includes also the prevention and security measures in addition to the Follow up by the Law Enforcement Agencies (LEAs)

**PREVENTION AND SECURITY**

Most Computer criminals thrive not on knowledge but instead blossom due to ignorance on the part of system administrator

Ankit Fadia.

Preventive measures as a part of legal control has been of legal control ;has been of crucial interest in the case of cyber crime as because the investigation evidence and trial in these cases are critical and difficult. Catching the hacker, or worm (virus) maker is a very complex process.

63 * Sup – 3 --------------- 1996 --------------- P– 172
64 * Sup – 55 --------------- 1985 --------------- P– 457
In the case of traditional crimes in real space, prevention is not possible in most of the cases but the Follow Up i.e. investigation - evidence and trial, is not so much uncertain as in cyber space.

Network security is essential for the protection of valuable information resources of the cyberspace. The intruders collect information’s from ISP, Net surfing and the chat rooms and also by scanning the target network or system. “Most computer criminals thrive not on knowledge but instead blossom due to ignorance on the part of system administrator”. *65

The system administrator (sysadmin) is required to look into the security issues and vulnerabilities as routine work.

The security measures to prevent and/or to make early detection may be (a) employing technical measure like electronic devices and surveillance and circumveption (test hacking) etc. (b) controlling physical access and human security “Security is a continuous process that is concurrent with innovations in technology. The basic rule pertaining to security are always the same. When some thing is secure, it means that it is safe from unauthorized access and modification”. *66

“Various parts of the total security arrangement thus relates to Logon Security, Communication line Security, Administration issues, Auditing and Human Security.

Various types of security incidents may happen such as Intrusion (by outsiders and insiders) Quiet Intrusion, Defaced pages, Errors and Omissions, Fraud and Theft, Malicious Code (virus, Trojans) etc. An incident refers to a situation in which the occurrences of an event either damages or has the potential to damage a resource. An incident in a computer related environment refers to an event that has an impact on the security of a network. “.............. All such incidents can be serious threats to the systems and networks of an organization. Although the actual damage caused by these incidents can’t be predicted, the damage by security incidents can range from disrupting work on a computer to harming the computing capabilities of large networks”. *67

Now the security incident thus relates to many issues and forms such as while an individual taking the access, or by the lawful user, or a client, or from network, or server, or even from the data input, or through a remote access or from the Internet itself. And the gravity of the incident may vary widely of which a rating or gradation has been developed by Computer Emergency Response Team (CERT) “The computer Emergency Response Team (CERT) at Carnegie Mellon’s a Software Engineering Institute rates Internet Security breaches on a Scale of 1 (the lowest) to 10. Historically, there was just one ‘Level-9’ event per year. The Melissa virus was a level 9 alert it was the fastest growing virus in history, forcing the shutdown of servers around the world. This is no longer the case; there’re many such events per year now”. *68

66 * Sup – 33 2003 P – 239.
67 * Sup – 14 2003 P – 327
68 * Sup – 1 2001 P - 299
The security issue in Internet and wireless communication are different to some extent. And the risk of access is greater in present wireless systems. The data moves from client mobile phone to WAP (wireless Application protocol) gateway and from this gateway to the web server. In side the WAP the wireless code (WML) is translated into Internet code (HTML). This is said to be unprotected from hacking. "WAP gateway bridges the wireless and wired Internet ........... A potential paradise for a hacker. He can hack into WAP gateway, gain access to the operating system ..... and install a sniffer program that captures the unprotected stream and save it to a file". * 69 The technical security involves the use of various technical devices program to detect intrusions, Intrusion Detection Systems, (IDS) Log files, Firewalls. However "It is nearly impossible to configure a firewall or create a network which is 100 percent foolproof, without compromising on the services that the network has on offer". * 70 The technical measures are to be supplemented with human security and surveillance. However hackers have their own methods to protect the resources. "............ because the hackers use free software, they can examine for security problems and they fix their own systems as soon as loopholes are discovered". * 71

B HUMAN SECURITY :

The access to the vital computer systems or terminals are the weak spots for any and every type of computer crimes so the physical access to the machines are controlled regulated and recorded. "Human security regulates the assignment of access to networked systems. It is the specific goal of human security to deny access to unauthorized users, to make different the compromise of secured systems and to provide criteria upon which potential users are judged as to whether access will be granted or revoked". * 72 Many security incidents i.e. crimes originate from the employees, insiders and high officials as root level security breaches.

A regular system of surveillance, audit and tamper proof log file are also part of security management.

The I T Act gives derailed provisions on security under the IT Security Guidelines framed under Rule 19(2) of the Act. The Guide line provides for Information Security Programmed U/s.2, physical and operational security U/s. 4; system integrity and security measures Access control Password Management. User Management etc. U/s. 6; Measures to handle computer virus U/s. 11; checking of system software U/s. 15; Network Communication Security U/s. 22; Emergency Preparedness U/s. 23; Security

70 * Sup – 65 ------------- 2003 ------------- Preface.
71 * M. Strebe & Ors – Firewalls – 1999 - Sybex Inc USA ----- P – 247
incident Reporting and Response U/s. 25 etc.

The I T Act also provides some more security and preventive measures under the security Guidelines for Certifying Authorities:- The Guideline provides for System Security Audit Procedures, Types of events recorded, Monitoring and Audit Logs, Login and Log of attempts etc. U/s. 9; Compromise and Disaster Recovery, Incident Management etc. U/s. 11; Key Management U/s. 18 etc.

(C) Some security sites:-
- http://www.cert.org
- http://www.cs.purdue.edu/coast/
- www. emergency.com/tech page.html
- http://www.web-police.org
- http://ciac.llnl.gov/ciac
- www.scamwatch.com
- www.microsoft.com/security

(D) For some software resources:-
- www.spammer.slammer.com
- For-e-mail filters - .............
- http://www.panix..com /e-s pa m .html.
- For minor protections ---- www. cyber angel .com.

5.6.1 DETECTION AND COMPLAINT

The process of legal control may be said to start with the detection of any security incident of Network or offensive material in the market like pirated software, (access device, application program etc). In case of cyber crimes however the detection of any security breach or intrusion is kept undisclosed for many reasons. Only a few cases come to light. This under reporting is a serious flaw in the process of legal management. “The true extent of computer crime is still unknown. Most organizations will refuse to share information about computer crime with law enforcement. And for every system penetration or instance of unauthorized use discovered, there are probably ten or more left unnoticed”. * 73

73 * Sup – 2 --------- 2000 ----------- Foreword (2).
The Computer Security Institute (CSI) San Francisco published a survey report*73A in 2000 which provided that 32% of the respondents had no knowledge whether they have been victim of unauthorized access causing addition alteration of data or downloading thereof. However many of them detected a wide range of cyber attacks and abuses such as 25% of respondents detected system penetration from the outside, 27% of respondents detected denial of service attacks, many of them detected employee abuse of Internet access privileges as downloading pornography or pirated software or inappropriate use of e-mail systems, computer viruses etc. Thus “According to CSI, the survey’ confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting”. * 74

In most cases of cyber crimes like intrusion, DOS, spamming cyber stalking, etc. the victim is required to make a complain with the Law Enforcement Agencies (LEA). But in case of software piracy, virus and worm related offences a suo-motu intervention, and recording are necessary by the LEAs.

The security incident as to computer content can be detected by using Intrusion Detection system (IDS), and computer auditing, and forensics. Every access to the computer database (no. of hits) can be detected and recorded and can be used as evidence.

Case: United States - V - Czubinski – (1st Cir. 1997)
The employee Czubinski accessed databases of his employers protected databases using the password and access code given by the employers to be used for some other business. The access was revealed and proved by the forensic audit of the computer concerned.

73A* - Infra74---2002 ---P – 44
5.6.2 JURISDICTION

The law of jurisdiction for the purposes of cyber crime will be (1) the standerd or conventional law as the first consideration i.e. “Territorial as a general rule the jurisdiction of the English Criminal Courts is confined to offences committed in England and Wales or the adjacent territorial water or on a British ship or British controlled aircraft. But there are important exceptions...Unless a statute expressly confers jurisdiction in respect of offences committed abroad, such offences can’t generally be tried by English courts, Which exercise criminal jurisdiction on the territorial principle over all offences committed in England, whatever the national of the accused may be and usually do not claim jurisdiction over offences committed abroad, even if they are alleged to have been committed by a British subject resident in England at the time of the trial”.*75

The law of extradition becomes relevant in the case of trial of foreign national in criminal trials. The problem arises of course in the cases where the concerned state parties have no Extradition Treaty. But in cyber crime the situation has been complicated due to frequent cross border offences. In this respect the civil rules of jurisdiction i.e. minimum contact, stream of trade and commerce, personal jurisdiction etc. are being discussed as solutions.

(2) Incase of cross border crimes involving multiple national territory the victim state will have personal jurisdiction on the accused. And the law of extradition will be applied to try the accused in the state of the victim. In absence of Extradition treaty, the trial depends upon dual criminality i.e. both or all the countries to have same criminal law as to the criminal liability of the actor in respect of the act in question.

In United States however some attempts have been made to assume extra territorial jurisdiction on the defendants.

In US v Thomas -1996-

The Tennessee court assumed jurisdiction on the defendant, a California resident for running a pornographic websites. Some other cases :- Hearst Corp- Vs - Gold berg , - 1997 WL 97097 (SDNY . 1997 )

Minnesota -v -Granite Gate Resorts 1996(Nevada)
CompuServe-Vs-Patterson-89F.Ed.1257 (6th cir.1 996)
UK law - The Computer Misuse Act -1990 provides U/s 4-9 that any offence having some significant link in the home country will be sufficient to assume jurisdiction on the issue

In Singapore - The Computer Misuse Act -1998 provides for imposing the criminal jurisdiction U/S -11 where any offence committed in Singapore or involved any computer, program or data, for the time being in Singapore at the material point of time.

*75 -Cross & Jones --Introduction to criminal law -1976--Butterworth & Co—P--405
The IT Act in India provides for territorial as well as extra territorial jurisdiction. s/1 (2) of the Act provides for assuming jurisdiction over crimes committed in India and it applies also to any offence or contravention there under committed outside India by any person.”

The law in India as to offences committed outside India by any foreign national will be liable to Indian. Criminal jurisdiction if the offence involved any significant material like computer or network situating in India. U/S.75 of the Act. “In this emerging scenario cyberspace which was initially thought to be a borderless medium devoid of graphical distinctions is slowly being fenced by electronic frontiers by means of cryptography and geographical location tools. This facilitates the application of traditional theories of jurisdiction to cyberspace.”

76* T.K Viswanathan (Member Secretary -Law Commission of India)- Souvenir -2-Intl-Conference on I/L- Oct -2002-Indian Society on I/L.
It is the duty of the state to prosecute and punish the criminals generally and the law enforcement agencies take initiative to prosecute the offenders in the court of law.

Prosecution actually sets the criminal law in motion against the offender and it presupposes detection reporting and /or complain to the LEA who make investigation to collect primary information as to the offence just sufficient for the case to be made out. “In cases where a crime is suspected the information is handed over to law enforcement authorities. When this information is transferred from person to person before being offered to the court as evidence these transfers must comply with the legal doctrine of chain of custody in which it must be shown that the evidence presented is exactly that which was taken from the crime scene.”*77 In cyber cases involving unauthorized access the intrusion detection, report, forensic audit and login information are relevant. Hence these are to be collected in electronic devices and requires to be protected under the system of chain of custody.

The criminal act and the intent must be proved beyond reasonable doubt. “..... the advent of network computer has created unprecedented opportunities for the anonymous perpetration of crimes. In fact, law enforcement exports perceive that the two most difficult problems they encounter are (1) establishing the identities of the alleged perpetrators, and (2) establishing jurisdiction over the alleged act of the perpetrators”.*78

In crimes like obscene website, cyber-gambling, fraud ,extortion ,theft, software piracy -the situation is somewhat different. Such as in spamming, the ISP- monitoring is essential but in cyber stalking (harassing) a long watch, trap and trace are necessary.

77* sup-1 ----2001----p-325
78* sup-1 ----2001----p-302
Investigation in all criminal cases is conducted to collect relevant information and evidence to prove the offence alleged. So investigation in cyber crime, as usual is directed to collect and to keep, the evidence in electronic form. This involves search and seizure, computer forensics, interception, decryption, password recovery, track and trace, ISP monitoring, traffic analysis etc. and also including human intelligence reports. The LEAs are also required to recover password, encryption keys to collect evidence. But the recovery of key or password in many cases can’t be made at all. So in the US, personal cryptography is considered undesirable, though it takes away the right to privacy of the Netizens. The search and seizure by LEA affects the rights of the people and hence the right to privacy requires to be protected in all cases of search.

In Kath v United States – 389 US 347 (1967) Held that search is constitutional only if it does not violate reasonable expectation of privacy. So in case of cyber crimes also the rule is equally applicable as was held in –

* United States V Barth – W D Tex 1998
* United States V Blas – E D Wis. Dec. 4, 1990
* United States V Reyes – SDNY 1996
* United States V Lynch – D VI 1995
* United States V Chan (ND Cal 1993)
* United States V Slanina (5 Cir. 2002)
* United States V Runyan (5th Cir – 2001)
* United States V Carey (10th Cir 1999)
* United States V Gorshkov (W D Sash, 2001)
* United States V Lyons (10th Cir 1993)

The computer forensic experts, cyber sleuths, are specialists who can discover relevant materials and information by examining the deleted files, disks, zip disks hard drives etc. This includes recovery and reconstruction of the data and communication found on the system or transmitted through ISPs.

Search and seizure are conducted to collect evidence of crime. But the search and seizure must not be excessive and must be according to law. “The process of gathering this evidence by officials is known as a search and seizure and is governed by the Fourth Amendment. Under the Fourth Amendment, the government in general is prohibited from
conducting a search or seizure unless it is done pursuant to search warrant". *79
In-United States V Hunter – 1998
The government was held liable to pay damages for excessive search, seizure and harassment caused to the person concerned. “Cyber crime investigations often involve electronic surveillance also. In computer crime cases investigators may want to monitor a hacker as he breaks into a victim computer system”. *80

Wide powers of interception have been given to the LEA to collect data information coming to and from the offender’s computer system, subject lawful requirement and rules of non-disclosure to third parties. The UK law through the Regulation of Investigatory powers Act ........ provides the power to intercept data communication with or without permission of the court.

The IT Act provides the power Investigation U/s. 28 & 29 by the CCA power of search and seizure U/s. 78,80 by a senior police official not below the rank of DSP. The controller of Certifying Authorities (CCA) U/s. 28,29 has the right to access to any Computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. In this regard the controller may take the technical assistance from the system administrator of the computer system.

The Act U/S/80 provides wide powers to the investigating officer (DSP or others) to conduct search in the computer kept in a public place, conveyance, hotel, shop accessible to the Public, and also to arrest the person concerned even without warrant, having reasonable suspicion of the commission (actual or attempted) of any offence under this Act.

The Official, thereby, following rules of the criminal procedure code will send the person before the magistrate without /unnecessary delay.

In India cyber police special cells have been established in Bangalore; Mumbai Delhi Hyderabad and Kolkata. “Over and above, the initiatives taken by the Central Bureau of Investigations (CBI) in co-ordinating with international agencies like FBI of US of America and arranging training for personnel of various state police forces have been widely appreciated”. *81 And the Computer Crime Investigation cell (CCIC) in Mumbai, traced and tracked Dr. Nuker (Anand Khare) and Da Libran (Mahesh Mhatre) who hacked the website of the CCIC (www.ccimumbai.com) in July 2001. The CCIC traced the server of the hacker’s computer from the log of their own Server Net 4 India. And ultimately reached the offenders through further investigation and interrogations.

79 * Sup – 1 ------------ 2001 -------------- P – 324.
81 * Sup – 47------------ 2004 -------------- P – 183.
(A) **Some Relevant Sites**

- www.forensics-intl.com/down.html
- http://www.pihome.com/pihome/index.cgi
- www.cyberpolice.ru
- www.cyberpolice.org
- www.crazytrain.com/seizure.html
- www.secretservice.org/electronic-evidence.html
- www.usdoj.com
5.6.5 EVIDENCE IN CYBER-CRIME

The entire subject of evidence in cyber crime has been a real challenge to the LEAs. However professionals from computer forensic experts, LEA and related sectors have created cyber-sleuths,(experts to examine deleted files) disks, zip disks, hard drive etc.

In cyber crime the physical involvement is so remote that the accused person can be reached only after a long chain of electronic records & evidence. And to establish a lawful link between the accused and the injury alleged becomes in many cases really difficult for the prosecution. This becomes so complicated because of the intangible nature of the electronic evidence. In many cases, therefore, the prosecution prefers the accused to plead guilty, especially in the offences involving multiple national jurisdictions. One very notable problem of digital evidence is that it has a short life span, cant be preserved for long years, “Digital is a problem, Digital storage media-floppies, compact discs, whatever don’t have a long life span, a few decades at most. Digital storage is an all or nothing proposition.“ * 82

Doctrine of Chain of Custody:

The important issue in preserving and producing protected electronic evidence has been the central question. “In cases where crime is suspected, the information is handed over to law enforcement authorities. When this information is transferred from person to person before being offered to the court as evidence, these transfers must comply with the legal doctrine of ‘chain of custody’, in which it must be shown that the evidence presented is exactly that which was taken from the crime scene. This becomes complicated by the fact that such evidence is easily altered and if this is so the evidence may not be admissible. The gathering and preservation of computer evidence is indeed fraught with difficulties. " * 83 The evidence may come out by monitoring the networks used by the hawks and also from the testimony of other hackers. “Indeed law enforcement realized that information that catches hackers and allows for prosecution is not going to be computers, disks or stereo cable, but instead the most valuable information will usually come from other hackers. Most hackers who are caught and / or sentenced are caught as a result of being turned in by another hacker." * 84

Once the crime incident is reported to the LEA-they take the initiative to collect information followings the steps like preparation (concerned forensic tools to be licensed one etc.), (Snapshot of actual evidence,( the place), Transportation (secure packing), preparation for Examination etc. “one of the most important characteristics of the cyber evidence is its global reach-----Department of Justice, USA advises the US law enforcement agencies that they should only make direct contact with an ISP located in another country, only with a (1) prior permission of the foreign government (2) approval of DOJ’s office of the International Affairs (OIA) or---(3) other clear indicia that such practice would not be objectionable in that country. “ *85

82* G.S. Hunter - Preserving Digital Information-2000-Neal Schuman NY-----P-1
83*Sup 1 ------------------------2001------------------------P -325
84*Sup-4-----------------------2000------------------------P-24
85*Sup-47---------------------2004------------------------p-206
In case of cross border offences International co-operation is a must for the crime investigation and evidence collection.

The UN Model Law (UNCITRAL) 1998 and different national legislations like UK, USA, Australia, Singapore etc. have provided for the legal recognition and admissibility of electronic evidence provided it is kept following a secure method.

The US rule of admission of computer records has two important points. The first one says that the evidence must be a part of records of regularly conducted transactions and routine procedure. “The second rule of admissibility of computer records in US is based on the assumption that they are hearsay evidence....However this is not a very happy situation, since the very definition of hearsay evidence is not applicable to a computer recorded document, unlike a document entered by a human being. There are many system generated documents such log files and these are not mere hearsay but concrete evidence of a happening.” *86 The computer generated document or information on the basis of some actual transaction may have better evidentiary value.

Case:-- Peope v Howwko (IIIL-19895)

The relevancy of routine procedure and regular transactions has been upheld in different cases:-

*United States v Salgado-(6th Cir. 2001)  
*United States v Cestnik (10th Cir 1994)  
*United States v Good Child (1st)  
*United States v Moore (1st Cir. 1991)  
*United States v Briscoe (7th Cir. 1990)  
*United States v Catabran (9th Cir. 1998)

The Information Technology Act also provides legal recognition of soft evidence or electronic evidence u/s. 4 of the Act. And also provides for retention of electronic record u/s. 7. The Indian Evidence (Amendment) Act-2000 also provides for Admissibility of Electronic Records u/s. 65. subject to some safeguards or conditions – as to regular and normal functioning of the computer etc. The General Clauses Act provides u/s. 3(65) that writing includes a printing, lithography and other modes of representing or reproducing words in a visible form. “The confusion arises when the computer is turn off.” *87

(case - * United States v Russo – us 1157 (1974) -- computer printout of medical record held valid. * Monotype Corporation v International Type Face Corporation (9th Cir. 1994) -- E-mail message not admitted holding that it was not a part of regular transaction.).

86 * Sup 47 -------------------------2004------------------------P -209
87 * Sup 30 -------------------------2001------------------------P- 78
5.6.6 TRIAL, JUDGMENT AND CONVICTIO

The general rule of criminal trial requires higher minimum proof for conviction. In Common Law countries, the burden of proof is on the prosecution To Protect the innocent from false and malicious prosecution in collaboration with law enforcement authorities and the legal system, perjury, corrupt lawyers and Judicial negligence, the rule of strict proof beyond all reasonable doubt is applied. "The consequences of conviction of a crime can be very terrible; that a guiltless man should suffer them has at any rate in the past, seemed to ordinary people to be a monstrous disaster. It is true that a strict application of the rules must occasionally enable a lucky wrongdoer to elude justice, and this may cause feelings of irritation. But these should not be allowed to obscure the social wisdom of the ancient adage that it is better that ninety-nine guilty men should escape than that one person should be unjustly convicted." *88 It is really a very sorry state of the legal system if any innocent person is convicted because as one offence (real) invites another offence of punishing and injuring an innocent man.

Crimes in cyberspace are so remotely committed that it is a difficult problem for the prosecution to establish a link between the offender and the commission of the offence. Especially when the techniques such as looping, remailing, erasing tracks, hidden filing, etc. are applied by the offender "While it is the hacker's body that must be found, identified and ultimately prosecuted, the relationship of hacking to the law has become curiously incorporeal in another sense. The most common legal indictment against a hacker is possession of counterfeit, unauthorized and stolen access device. Literally this refers to password." *88 A

Thus in US Law-- the possession, creation and transfer of access device has been made criminal offence u/s. 1030 U S Code. "The role of prosecutors and the defense lawyers in evaluating and presenting such evidence in a court of law can't be overemphasized." *89

The IT ACT provides for a separate trial by Adjudicating Authority u/s. 46 & 47 and Cyber Regulations Appellate Tribunal (CRAT) U/S. 48,55,57, 58,59 & 60 of the Act in rule of civil procedure. But the other crimes described u/s. 65 Tampering, s/66 Hacking and s/67 obscene material, s/70 Protected System access, have been kept under the prevailing system of criminal jurisdiction. The penalty system in India has been the same old form of fine and/or imprisonment, but it may be added with community service. Probation, or other soft methods.