CHAPTER – III

A Study of Cyber Crimes

3.0 History of Cyber Crimes

3.1 The White Hats:

The opportunity for creative computer hardware and software invention became available in the 1960s and 1970s through the academic explorations at the all-male Massachusetts Institute of Technology (MIT), Tech Model Railroad Club (TMRC). The TMRC was formed in 1946 and continues to this day as an actual model railroad club. The original members used their skills learned at MIT to employ advanced control systems and became the first white hat hackers.

During this period, the word hacker began to represent a technologically focused individual and the term was applied to those who spent time crawling under the railroad tracks at the Railroad Club facility with the primary objective of connecting switches to relay with cables. Back in the early 1960s and 1970s, a “back” meant a prank of the kind that the student and the MIT faculty played on their school or on their rivals as wrapping the entire root in tin foil. A “good hack” would have been some creative exploit that would have impressed observers to remark “How in the [heck] did they do that?” Eventually, the term evolved from meaning of any prank to a computer prank the students started to work more closely with computer systems.

Famous white Hats (a term borrowed from black – and – white early western movies that indicated the heroes, or good guys of the story) at MIT included Alan Kotok, Stewart Nelson, Richard Greenblatt, Tom knight and Bill Gosper. These early hackers were known to work in the lab for 30-hours-plus shifts and found the primitive computers so fascinating that they forgot about everything else while they were working on them. They even fought themselves to pick locks in the MIT computer science building to gain access to the computers after hours. From the white Hat’s perspective, this lock-picking was not criminal activity because they felt they were simply putting all available equipment to its best use. In short, the white hats


believed that computers should not be locked and should be available 24 hours a day.
These early hackers were not criminals, but highly talented programmers committed to finding novel solutions to difficult problems. If the type of software or hardware they wanted was not available, these hackers would develop it. The search for new solutions created a hacker community of people who began to share computer code while building an open and freely accessible body of knowledge among peers. It was the sort of intellectual environment that is afforded to academics and is protected by academic freedom and tenure.

After the 1960 and 1970s, the cyber frontier blew wide open, with white hat hackers across the United States exploring and figuring out how the wired world worked and paving the way for incredible growth along the information superhighway.

3.1.1 The White Hat Ethic

The White Hat Hacker Ethic, perhaps best expressed now in Steven Levy’s 1984 book was the guiding light for positively motivated white hat hackers back in the 1960s. In fact, the Hacker Ethic is said to still be the backbone of creative hacking today. The hacker Ethic includes two key principles formulated in the early days of the MIT hacker escapades.

1. Access to computers – and anything that might teach individuals. Something about the way the world works – should be free.
2. All information should be free.

In the context in which these two principles were formulated, the computers were “research machines” and the information was “software and systems information”. The cautionary theme behind the white hat Hacker’s Ethic is that information hoarding by government and other authorities is not only inefficient, but it also retards the evolution of technology and the growth of the information economy.

For other tenets described by Levy are also referred to by present day White Hats as being integral to the motivations behind their positively predisposed behaviors. These include the ideas that (Levy, 1984):

---

3. Supra 2.
1. Authority should be mistrusted and decentralization of information should be promoted.

2. Hackers’ status in their community should be judged by their hacking prowess, skill sets, and outcomes – and not by irrelevant criteria such as formal educational degrees, age, race, or societal position.

3. Both art and beauty can be created on a computer.

4. Computers can, indeed, change ones’ life for the better.

Richard Stallman, an elite and highly recognized hacker in the computer community who worked at the MIT Artificial Intelligence (AI) Laboratory during the 1970s and who was the founder of the Free software foundation, speaks to the notion of the hacker Ethic.

“I don’t know if there actually is a hacker’s ethic as such, but there sure was an MIT Artificial Intelligence Lab ethic. This was that bureaucracy should not be allowed to get in the way of doing anything useful. Rules did not matter – results mattered. Rules in the form of computer security or lock on doors, were held in total, absolute disrespect. We would be proud of how quickly we would sweep away whatever little piece of bureaucracy was getting in the way, how little time it forced you to waste. Anyone who dared to lock a terminal in his office, say because he was a professor and, thought he was more important than other people, would likely find his door left open the next morning. I would just climb over the ceiling or under the floor, move the terminal out, or leave the door open with a note saying what a big inconvenience it is to have to go under the floor, “so please do not inconvenience people by locking the door any longer”. Even now, there is a big wrench at the AI Lab, titled, “the seventh-floor master key” to be used in case anyone dares to lock up one of the more fancy terminals.

3.2 The Black Hats

Black Hats in the United States, like the white hats, the term Hats also originated in the United States from black – and – white western movies and was meant to represent the villains, or bad guys. Though white Hat hackers, generally place the Hackers’ Ethic on a rather high intellectual plane, honour it, and expect it to

---

be honoured by others in the computer underground, Black Hat hackers are typically not committed to or behaviorally ruled by the Ethic. Though there is considerable debate about when the term ‘Black Hat’, or ‘cyber criminal’, was actually coined, reports seem to indicate that. John Draper (ak-a capn crunch), user of a cereal box whistle that generated a 2600 Hz tone when blown, was likely the first alleged “criminal” cracker to come to the attention of the popular North American media.

The year was 1971, and the stimulus was journalist Row Rosenbaum’s article in Esquire magazine on Draper’s amazing whistle – blowing breaking exploits, which not only allowed Draper to make free telephone calls but also eventually landed him in prison. By covering one of its roles and blowing through the capn crunch whistle (a trick he had learned from some friends who were blind). Draper could produce a tone with the frequency of exactly 2,600 Hz. This happened to be true that American Telephone and Telegraph (AT & T) and other long-distance phone lines were available. If either phone that was party to a call entitled this tone, the switch controlling the call would be tooled into thinking that the call had ended and all billing for the call would stop. In short, whistle enabled Draper and some of his friends to call each other long-distance for free.

While incarcerate, Draper was approached of mafia members wanting to utilize his unique skill set. After Draper refused to co-operate with them, he was severely beaten. Upon his release from prison, Draper was approached by an old friend Steve Wozniak, developer of the Apple II Computer. Wozniak asked Draper to stop breaking in favour of computer programming and there began a more positive era in Drapers life. It was John Draper who wrote Easy writer, the word-processing program sold in 1981 by IBM with their personal computers (PCs). This story has a happy ending in that cap’n crunch eventually became one of the first high-tech millionaires. A little-known fact, about this once criminal breaker is that he was honorably discharged from the United States Air Force in 1968 after serving in Vietnam.

Since Draper’s time, there have been countless young, creative crackers who are generally self-taught or who are taught by colleagues in the computer underground. These crackers exploit various computer systems. Sometimes they get

---

caught and are imprisoned; other times, however, they commit their exploits without being caught after note researchers Schell, Dodge and Moutsatsos (2002), after age 30, these crackers being to embrace the Hacker's Ethic and to contribute positively to society. Many times, cracking and phreaking exploits become a means by which troubled and often talented young minds act out their anger and frustration. Rather than working through their issues, perhaps with mental health experts, troubled young crackers often turn to their computer of a means of escaping reality. Unfortunately, they may use their computers to commit crimes.

Chamberlin's speciality is security and intrusion detection, and today with the modern growth in cyber crime, his computer skills are in high demand. Chamberlin claims to have had his own tense "experimental" cyber moments. As a teenager in southern California, he learned programming using one of the first personal computers, a Timex Sinclair. He purportedly experimented with electronic bulletin Boards and the ARPANET, the early Internet established by the United States Department of Defense exact what he did as an experimental adolescent he does not say? But he remarks that he was glad he was a juvenile, giving the impression that he was likely cut from the same cloth as John Draper. Chamberlin insists, however, that he never actually got into legal trouble. Chamberlin's story illustrates that though he may have had some Block tendencies in youth, he eventually realized that his talent could be better utilized as a white hat.

3.2.1 Black Hats in Great Britain

Elsewhere around the globe, the term cyber criminal took a bit longer than it did in the United States to find its way into the press lime light. In Great Britain in April 1986, for example, the term criminal hacker was eluded to, triggering the public's fears about cyber crimes, with the convictions of Robert Schifreen and Steven Gold, highly profiled crackers of the BT prestatl service.

In 1984, BT prestatl operated a text information retrieval system that was accessible over the public Switched telephone system by means of a modem. The electronic mailbox information could be retrieved and viewed on a personal computer or on a television screen. Although some of the information was available to users at
no charge, other information required a fee. To access the information system, users were each given a unique Personal Identification Number (PIN), much like those used by customers today to access finds from automated banking machines.

The cyber crime of Sohifreen and Gold was cracking into the system and leaving a greeting for His Royal Highness the Duke of Edinburgh on his British Telecom prestal mail box (an early phone voice mail system). The two were convicted on a number of criminal charges under the British Forgery and Counterfeiting Act of 1981. However, in April, 1988, their convictions were set aside through an appeal to the House of Lords. The reasoning of the judges hearing the case was that the spirit of the Forgery and Counterfeiting Act was being stretched to an unacceptable limit and the Act was considered to be inappropriate for application in cracking related circumstances.

Shortly thereafter in July 1988, the British press reported the cyber crime exploits of Nicholas Whitley, known as the Mad Hacker. In May 1990, he was one of the first crackers in Britain to be convicted under the Criminal Damage Act of 1971. Whitley was given a custodial sentence for cracking into the computer system at the Universities of London, Bath and Hull, causing them to crash (Mulhall, 1997a).

The cases of Schifreen, Gold and Whiteley were instrumental in bringing cyber crime into the public arena in Britain. Moreover, they were instrumental; they were instrumental in prompting the passage of legislation specifically geared to computer hacking, Michael Colvin, a member of parliament, worked with the Department of Trade and Industry to get a bill through the British parliament that eventually translated into the Computer Misuse Act of 1990 (Mulhall, 1997a).

3.3 Emerging Fears about Cyber terrorism

From 1971 through 1998, both ‘White Hat hackers’ and Black Hat crackers’ received media air time for a variety of cyber exploits. Then in 1999, a new cyber-related fear emerged. Two professional soldiers in China’s People’s Liberation Army proposed a new way of waging war by using terrorist attacks and cyber attacks on critical infrastructure as a way to key a super power adversary reeling. But it was unclear whether this threat was an emerging real one just fiction.

In a foreshadowing media story that appeared in February 2000, John Serbian, the CIA’s information issue manager, said in written testimony to the United States Joint Economic Committee. “we are detecting with increasing frequency, the
appearance of doctrine dedicated cyber warfare programs in other countries, we have identified several, based on all-source intelligence information, that are pursuing, government sponsored offensive cyber programs.\textsuperscript{7}

3.4 WHAT IS CYBER CRIME?

'Cyber crime' is a rather pretentious expression to refer simply to the use of computers by criminals. It is a crime by criminals by exploitation of computer and Internet. Cyber crime is a new form of crime now being committing by criminals of the modern times. It has gained very fast recognition demanding immediate attention, follow-up and combat. The legislature, judiciary and the law enforcing authorities have to face this new challenge.

There is, after all, nothing very new in the adoption by criminals of new technologies cases of bank robbers using portable radios to intercept police transmissions and more recently the utilization of mobile cellular phones for evading police detection provide obvious examples. The technologies have been an increasingly important aspect of crime detection including the use of a wireless signal.\textsuperscript{8}

B.B. Nanda and R.K. Tiwari, define Cyber Crime: A new generation of crimes has cropped up by the advent of Internet, computer hacking, software piracy, Internet pedophilia, industrial espionage, password breaking, spoofing, telecommunication frauds, e-mail bombing, spamming, pornography and the availability of illicit or unlicensed products and services are offences that have already made their mark.\textsuperscript{9} The phrase “computer crime” or “computer misuse” has no precise definition and tends to cover a multitude of “computer misuse” has no precise definition and tends to cover a multitude of computer related offences ranging from unauthorized access to computers and computer stored material, causing damage to computer held information, trafficking in passwords and hacking-friendly technology, manufacturing and selling pirated copies of software and transmission of pornographic material.\textsuperscript{10}

\textsuperscript{7} Bermade H. Scbell and Clemens Martin, Cyber Crime – A Reference Hand Book – Edn. 2004, p. 4-10.
\textsuperscript{10} India carr, India joins the cyber-race : Information Technology Act, 2000).
electronic media. The electronic media is comprised of the information network or the Internet and the online computers.

Electronic commerce crime (like the theft of hundreds of thousands of credit card records) threatens the Internet boom. Electronic espionage like the theft of biotech secrets stored in digital files).............. Infrastructure attacks (like an assault against a nation's power grid) threaten the safety and well-being of whole populations. Other cyber crime, such as identity theft or cyber stalking, strike at indicitizens, exposing them to financial psychological and even physical°°.

To understand cyber crime as a significantly new phenomenon, with potentially profound consequences, it is necessary, it recognize, it is a constituent aspect of the wider political, social and economic restructuring currently affecting countries world wide. In particular, the process of economic globalization, which are being facilitated by the new ICTs not only provide the opportunities for the profitable development of international informational markets but also simultaneously raise the specter of new criminal activities arising to exploit them. The very technologies which unable multinational corporations to do business more easily and challenge the individual controls and regulations of nation states also offer the prospect of globally organized criminal networks. Moreover, the free flow of uncensored, information on electronic networks and websites is as attractive to insurgents and extremist groups as it is to dissidents proclaiming their human rights.

Cyber crime can be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by the new ICTs. The global connectivity of the Internet; for example, makes it much easier for criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing organized crime to use move sophisticated techniques to support and develop networks for drugs trafficking, money laundering, illegal arms trafficking, and smuggling the like. For hackers with the requisite computer skill, a large market exists for security and trade secrets which can be accessed and transmitted electronically. Furthermore, the many-to-many communication which is an essential feature of the Internet enables the

13 Supra 8, p. 2.
production and world wide dissemination of information and knowledge which could be potentially harmful threatening or liable to incite violence.

The nascent threat of cyber crime to affect national and international economics, security and social and political relations provides a serious challenge to the future roles and practices of law enforcement agencies and security services. A flexible communications system designed to withstand attack by means of rerouting messages has also provided difficult for governments to control. Sources of illegal activity often require advanced computer skills to be detected as a consequence of their anonymous character.

The transforming qualities of ICTs make it increasingly difficult to distinguish between warfare terrorism and criminal activities. Extremist political groups, for example, may engage in all three. The trial of Timothy Mc Veigh for his part in the Oklahoma City bombing provides perhaps the most dramatic illustration to date. Also, national security is vitally dependent upon economic security. A country in the post cold war period may be more under threat from economic espionage than nuclear assault. The use of ICTs by non-government organizations and international criminal organizations will therefore clearly have an increasingly important impact upon the functioning of law enforcement and security agencies in the information age.

3.5 DIFFERENT TYPES OF CYBER CRIMES AND THEIR MODUS OPERANDI

The dark side of cyber space has some difference from the real space in that the differences 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 motivated 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 computers, such as distribution of pornography. Other crimes are solely the product of phenomenon of the Internet”\(^\text{16}\). The Internet has provided some special advantages to the 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), violations of intellectual property right. “The kinds of crime instigated on Net are indeed many and varied. Some of the


\(^{15}\) Supra 8, p. 3.

\(^{16}\) Yatindra Singh (Judge Allahabad High Court) – Journal of India Law Institute – 2001 – P – 301.
The other mode of computer crime are unauthorized access and damage to the networks and on-line computers by criminal hackers and some other like virus and worms. Denial of service ata

3.5.1 Types of Cyber crime

Social Engineering: - It is important to note that some deliberate attacks on computer systems originate in non-technical ways and use “social engineering” techniques that take advantage of naïve or inadequately trained employees. In other words, some cyber crimes are committed without much sophistication. The perpetrators simply capitalize on the “weakest links” in the system.

Social engineering describes the deceptive process whereby crackers “engineer” a social situation to allow them to obtain access to an otherwise closed network. Typically, the objective of the exercise is to get others – the weakest links – to reveal information that can be used to copy or steal data. For example, a cracker could talk a computer help desk employee with resetting the password on a stolen account. Once a password was obtained, access to the system by the cracker could be either permanent or temporary.

One of the most notorious social engineers in the computer underground went by the pseudonym of Susan Thunder. Susan Thunder was reportedly mistreated as a child and became a prostitute in her teens. In her spare time, Susan Thunder fraternized with various rock bands. She discovered how easy it was to get back stage passes for concerts just by calling the appropriate people and pretending to be, for example, a secretary at a record company – a form of social engineering. Susan eventually became an active phone phreaker, and with the non-famous cracker team of Kevin and Ron Mitnick, she broke into the telephone lines in the 1970s. Susan Thunder exploded the then popular myth that only men could enjoy the “pleasures” of cracking. Eventually, the team of three cracked into U.S. Leasing’s systems, deleted all of the information off one computer, filled the computer with messages like “F-YOUF-YOUF-YOU”, and programmed the printers to continuously spit out similar insults. Interestingly, among all the profanities were planted the names of Kevin and Ron.18

17 Supra 14 – p. 5.
security consultant Rumor had it that Susan Thunder was angry with Ron, with whom she was romantically involved, for finding a more socially acceptable girlfriend elsewhere (recall that Susan was a prostitute) when Ron and Kelvin were arrested. Susan was given immunity from prosecution in return for testifying against them. Later she referred to herself as a security expert and conspicuously demonstrated how she could break into military computers, using her well-honed social engineering techniques.

3.6 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 today 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." 20

3.6.1 Hacker and Cracker: Differences

Previously, the word hacker in Yiddish meant an inept furniture maker. In present day terminology, and particularly in media reports, the word hacker has now taken on numerous meanings. from a person who enjoys learning the details of computer systems and how to stretch their capabilities to a malicious or inquisitive

meddler who tries to discover information by deceptive or illegal means. A cracker is someone who breaks security on a system. The term was coined in 1985 by hackers angered at the journalistic misuse of the word hacker.

In recent years, the boundary between the meanings of the terms hacking and cracking has become blurred. In fact most media pieces reporting computer system intrusions today typically use the word hacker when the more correct term would be cracker. To which Hat hackers – the “good guys” in the computer underground – the Black Hats, or crackers, are the cyber criminals. The white Hats maintain that they are motivated by creative exploits into the cyber world, including the quest for knowledge or the need to find intrusion flaws by breaking into a computer system with authorization. The Black Hat crackers, on the other hand, commit crimes using a computer. There motives vary: getting revenge, sabotaging competitors’ computer system, stealing information or identities from others, and terrorizing selected targets.

By definition, cyber crime is a crime related to technology, computers and the Internet. The majority of publicized cyber crimes that concern governments, industry officials, and citizens world wide include:

- **Cracking**: Gaining unauthorized access to computer systems to commit a crime, such as digging into the code to make a copy-protected program run without a password or a valid license, string, flooding Internet sites and thus denying service to legitimate users, erasing information corrupting information, and deliberately defacing web sites.

- **Piracy**: Copying protected software without authorization

- **Phreaking**: Obtaining free telephone calls or having calls charged to a different account by using a computer or another device to manipulated a phone system.

- **Cyber stalking**: Harassing and terrorizing selected human and institutional targets using the computer, causing them to fear injury or harm.

- **Cyber pornography**: Producing and/or distributing pornography using a computer.

- **Cyber terrorism**: Unlawful attacks and threats of attack by terrorists against computers, networks and the information stored therein to intimidate or coerce a government or its people to further the perpetrators political or social
3.6.2 **EARLY HACKING**

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 in defense 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 of 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. In this age, the hackers were trying to guess the log on names and passwords from the first names, last names, names related to the family of users etc. and sometimes they were successful to guess the correct one (log on names/passwords) and break into the computer or time sharing systems.

In the 19th century rail board had been leased to Telegraph companies and again it was taken by telephone companies to develop long distance network. “The telephone system was the first global computer and it was legitimate political target”. The global telephone network had provided for tele abuse and telephone hacking called phreaking in the early second half of 20th century.

“In parallel to the computer hacking activities a new of hackers, phreaks came into action. Phreaks first accessed telephone networks by using hand held 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.”

---

22. Supra 18 – p. 4.  
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 National Semiconductor who went by the alias of Capt’n Curnch, is that granted access to AT & T’S long distance service”. John Draper, however, was arrested in 1972 for making and supplying blue boxes but he is said to train phreakers and backers while in prison also.

John Draper, however, was arrested in 1972 for making and supplying blue boxes, but he is said to train phreakers and backers 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 own phreaker counterparts in England in 1960s and 1970s to make free long distance calls, and to take other advantages. They developed Sleeper Box to create deceptive tones of variable frequencies like the Blue Box of John Draper to take back door 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 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 “cheese 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 cheese box to disguise the number at which they were actually located24.

In the next period the older equipment was being replaced with digital equipment, computer 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 security problem of course, all transactions with the computer are logged, but hackers have ways of hiding their activities ........".

In the last thirty years, phone hacking (phreaking) has merged with computer having....... There is a much variety of things hackers can do now. More equipment and software means there are so many more hacks needed to get into systems. Because most of this equipment can be purchased through independent companies it is very easy for a hacker to pose as customer ........... John Cap'n Crunch. Draper December 1999\textsuperscript{25}.

In the new age of computer telecommunication, the phone hackers equipped themselves with the knowledge of digital technology, "BB Nauda and Dr. R.K. Tiwari observe that 'Internet pedophilia computer network break ins, industrial espionage fraud, software piracy, e-mail bombing and spamming and the availability of unlicensed products and services are already making themselves felt'\textsuperscript{26}.

3.6.3 MODERN HACKING ;

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

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.

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 – IX, NT or the many flavors of Unix. Others will acquire software programming, take errors that they can exploit.27

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

In late 1990s some hacker used to operate are given below:

http://www.undergroundnews.com;
http://www.hacker.org ; http://www.kevinmitnick.com;
http://www.ucl.ru;

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 operation.

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 purposes or training purposes subject to the hackers own or permitted sites. “And now a days the media has been wrongly and outrageously referring to computer criminals as Hackers. They fail 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”28.

The computer managed telecommunication system in 1970s onwards gave the long arms to the hacking community. In 1997 Carlos Salgado of California hacked

27 Supra 23 – p. 7.
several media companies like World Wide Web and some ISPs. He accused 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 shall light on the dark side of the electronic commerce gold rush.”

The investigation of cases 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 pocket sniffer placed in the system to collect log ons. 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 situations. And ultimately Carlos SMAK was arrested with the CD-ROM containing about 1 lac credit card numbers in the San Francisco airport in 1997.

Chris Goggans in 1990s became notorious hackers and founded that 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 become a computer security professional in late 1990s. Sergej 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 Gstman(20) alias spy-ball, 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.cru). “Leshy is said to be accused of fabricating (and distributing) 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
from (http://www.computer.ru/forum/hackers). While the discussion proceeds, highly
critical views are being addressed to the security and cyber police bureaus"30.

Hackers usually prefer to form small groups and individual hackers is
generally uncommon. One such Russian group is RAF (Russian Anti Fascist Frontier)
generally engaged in spreading and upholding political views rather than committing
criminal activities. But another groups 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 Hack zone
(http://hackzone.ru) – which functions in close collaboration with a German team
“werewolf". The United Crackers huge (UCL – http://www.ucl.ru) was also engaged
in criminal activity where the above mentioned hacker, Leshy was an active member.

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 draw attention to their activities. Rather they wanted to remain
unobserved well as anonymous, because detection would mean their routes into a
system would be closed. This new breed of hacker broke into system to use them and
/or to view data they stored. This meant they weren’t in there ripping up databases.
The likelihood of detection was less, and this sort of hacker’s : intrusions could and
did continue for months on end”31.

Sometimes hackers use virus as a tool to dislocate the function of a computer
or computer system. And in this method the hacker in most cases 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 or
windows 98, the program allows unauthorized remote access of the machine”32.

The hackers exchange their views and show knowledge among themselves and
hence they run their own websites and attend conferences.

Some of the hackers websites are :
http://www.hacking.secret.com ; http://www.telehack.net ;
http://www.hackzone.ru ;

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

3.6.4 SECURITY SITES

The following are some sites which provide assistance and guidance in need against criminal activities in cyberspace.

http://www.infowar.com
http://csrc.nist.gov/
http://www.cast.org/
http://www.microsoft.com/security
http://www.sans.org

3.7 TAMPERING (SOURCE CODE)

All the digital data bases and source code-4S 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 programme".

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.

3.7.1 Malicious Code

These are commonly called computer virus, bug or work. In fact, these are carefully and intelligently written program. The machine realizes 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 own machine language or binary code and follows the long chain

---

of instruction step by step. The code writer, the programmer arranges the instructions on such a way that the machine becomes puzzled by trickily 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 a software program that can make copies of it ……….. The virus looks for a place to copy a clone. It can 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”34.

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 virus software resources : www.antivirus.com; www.av.ibm.com ; www.virusbtn.com .


3.7.2 SPAM

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 the 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”. It may be like make money with computer, work at opportunity”35.

To restrict spam anti-spamming software are the following :

1) www.spammersslammer.com
2) http://www.pankp.com/e-spam.html
3) http://www.ca-probate.com/aol/junk/html
4) http://com.primenet.com/spamking/slatinfo.html

Spam king /slatinfo.html. complain against the spamming may be made to the spammer’s ISP or to

: Abuse@aol.com
: Abuse@netcom.com
: Abuse@interamp.com

35 Supra 29 – p. 176.
3.8 **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 megabyte is sent to it, when the victim computer can but receive it and thus remains engaged solely to receive it continuously for hours and days together. Obviously the e-mail message contains nothing of value i.e., meaningless data stream. In 1996 a single hacker launched a denial of service attack against “panix – a New York Internet Service provider, for nine days, nearly putting them out of business and severally hurting their customers in the process. The distinguished researcher William Cheswick agrees that DOS is significant challenge facing the security community. The ISP, American online (AOL) 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 attack, fraggle and Smurf attacks.

The DOS attack broadly may be of two types, 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 address and the target computer will crash failing 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”.

The causes of DOS attack may be found in the very nature of the Internet System and Internet application softwares. 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”.

---

36 Supra 30 – p. XVI.
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, enter communication among different server 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”39.

Some of the information resources on the DOS attack –

- http://www.attrition.org/security/denial
- Attack tools – at www.packet.storm.security.com
- Protection tools at http://www.comsoc.org/socstr/tech.com/ntwork/IEEE

3.9 PORN WEBSITES

A very common problem in cyber space is the numerous 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”40.

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


In American Civil Liberties Union vs Reno 1996 WLG 5464 EDPA, Reno placed pornographic materials on the websites and ACLU brought an action against it. The court allowed injunction in the case. However the right to speech and expression was sought to protect indecent, not obscene communications as between adults.

The IT Act – 2000 provides the law u/s 67 on publication, transmission of obscene materials in the cyber space. The Act provides for a penalty of five years imprisonment and a fine up to one lakh rupees but for subsequent conviction the term may extend up to 10 years and a fine of two lakh rupees.

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

---

39 Supra 33 – p. 252.
40 Supra 32 – p. 292.
computer to know the movements of the child concerned. The site www.cyberangel.org/safety and privacy/chart html also provide filter programs.

Some resources for protection and guidance are :-

1. www.safekids.com
3. www.cyberangel.org
4. www.cdt.org

3.10 **CYBER FRAUD (SCAM)**

Cyber space being the mirror of the real space, and 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 citizens. “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.”

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 are :

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 connect 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 reports sites -

a. Internet Fraud Watch – www.fraud.org. Or 800.876.7060
b. Fax to S. Florida Task Force - - 954, 925, 1362
c. www.fraud.org
d. www.locus.halcycon.com

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.

---

41. Supra 31 – p. 280.
3.11 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 or posting in cyber space 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 or users sending harassing or threatening e-mail to other users”. 42

3.12 CRIMES ON THE NET

A statement by Neil Gallagher, a Deputy Assistant Director for the FBI, to the US congressional Joint Economic Committee suggested that the World Wide Web has allowed for an endless barrage of frauds, scams, intrusions and piracy. The kinds of crime instigated on the NET are indeed many and varied. Some of the most common would include the following:

Computer network break-ins. Typically these involve hackers breaking into computer systems and networks to steal data or undertake acts of sabotage such as planting viruses or Trojan horses. Some of the most significant threats to commercial enterprise come from industrial espionage which concerns the time – honoured tradition of spying upon ones competitors. The arrival of ICTs provides new opportunities for hacking into and obtaining information for sale about product development, marketing strategies and other trade ‘secrets’. The expanding value of the technologies themselves also offers significant bounties for those able to capture intelligence as a result of software piracy.

With electronic commerce rapidly becoming a major factor in national economics it offers rich pickings for criminals prepared to undertake fraudulence activities. According to Gallagher, in the USA the ten most frequent fraud reports involve undelivered internet and online services; damaged defective, misrepresented or undelivered merchandise; auction sales; pyramid schemes and multilevel marketing; misrepresented cyberspace, business opportunities and franchises; work-at-home schemes; prizes and sweepstakes; credit card offers something like half a billion US dollars may be lost annually by consumers through credit card fraud alone.

Computer systems are also susceptible to attack through the use of mail bombings, a process whereby software is designed to instruct a computer to repeatedly send e-mail to a specified electronic address. The effect of such a bombardment can be to flood the recipients’ personal account and thereby threaten to shut down the whole system. Furthermore, other software programs known as password sniffers can undermine the security safeguards of whole computer networks. The identity and password of network users can be monitored and recorded to enable impersonators to access restricted files and documents. A related activity known as spoofing also enable illicit access by electronically disguising a computer to resemble another.\footnote{Supra 7 – p. 5-6.}

3.12.1 Who are the cyber criminals?

Understanding who the new cyber criminals are, is not simply a matter of thinking about old crimes in a new ways. Cyber criminals, like cyber crime itself, are marked by a fundamental transformation in the way we think about the issue of crime and criminality. Acts considered criminal that merely happen to involve ICTs are of less concern than those which are made possible solely by the use of ICTs. For example, the use of a computer to defraud someone is no different than the use of a telephone or a face to-face conversation to defraud someone. What makes such crimes cyber crime is when the use of ICTs adds a significant element to the crime which would have been impossible without them. For example, using e-mail or the www to defraud hundreds of thousands of people, the use of the Net to spread information inexpensively, anonymously, or in great numbers all charge the fundamental nature of the crime being committed, not merely the means by which it is done.

Just as crime have changed with the growth of ICTs, so too have the categories of criminals who engage in such crimes. There are three basic categories in which we can categorize cyber criminals: hackers and phreaks, information merchants and mercenaries and terrorists, extremists and deviants.

3.12.2 Hackers and phreaks

Computer hackers and phreaks (telephone hackers) use ICTs to illegally enter computer systems, for the purposes of exploitation, information or curiosity. Their crimes, while illegal, are generally not intended to cause damage to data or to reap financial reward. Often hackers and phreaks will engage in pranks, such as rerouting
phone calls or rearranging web pages. While their actions may have financial consequences for individuals, corporations or industry, their primary goal is not to profit from their crimes. In many cases, hackers are out to find bugs or holes in systems to gain a reputation for daring hacking exploits, or to embarrass industry figures or people in positions of power. A small subject of those hackers, referred to as malicious hackers cause damage, delete or erase files, or make confidential information public. This group may also include hackers who use computer or telephone technology for minor fraud (using stolen credit card information to make purchases referred to as carding), those who write computer viruses, or those who shut down Internet websites or Internet service providers (known as denial of service attacks).

For the most part, these hackers are driven by a sense of curiosity and most of the damage done by this group is either unintended or incidental. Typical crimes include on-level fraud (usually related to attempts to gain access to computer systems by attaining password information, unauthorized access to computer systems and possession of unauthorized access devices such as passwords or access codes.

3.12.3 Information merchants and mercenaries:

In contrast to hackers, information merchants and mercenaries trade in the commercial sale of information, engaging in crimes such as corporate espionage and sabotage, sale and theft of identity information, computer and network break-ins, and large-scale software piracy. While they may use similar tools and techniques as hackers, information merchants and mercenaries are primarily driven by profit. Those involved in attaining and selling information often are hired by competing corporations or only themselves, former employees for the companies or agencies from which they gather information.

This group refers to anyone using ICTs primarily for the purposes of illegally reaping financial gain. This may involve illegal discovery or access to information illegally obtained information. Also falling into this category are those who use ICTs, such as cryptography, to hide disguise illegal activity as well as those who exploits ICTs for illegal financial gain;\(^{44}\).

3.12.4 Perceptions of cyber criminals Hackers, insurgents and extremist groups:

\(^{44}\) Supra 7 – p. 6-7.
The idea of cyber crime has, in many ways, become synonymous with hackers and hacking. Films TV and Science fiction novels have portrayed hackers as everything from data cowboys on the electronic frontier to digital vigilantes for hire in cyber space.

Hackers are perhaps the most easily identified group of cyber criminals and as a result they have come to represent in the media, in entertainment and in the popular imagination, the risks and dangers of new ICTs. Often, these risks and dangers are more imagined that real, but they do serve to reveal a great deal about public perceptions of the relationships between new media technology and crime. Specifically, hackers are often markers of the fragility of new ICTs representatives of the risks of new information technologies and the potential for danger. They also personify a new breed of out law, constantly challenging accepted definitions and ideas about technology, security and privacy.

Hacking, as pioneers on the ‘digital frontier’ find themselves at the limits of the law, in a space where commonly accepted notions of law and order become complex and uncertain. The most basic example that of trespass is utterly confounded by notions of virtual space. How can a hacker be accused of trespassing on someone else, property when his or her physical presence is located hundreds or even thousands of miles away ? It is a problem that ICTs introduce into the law which hackers exploit to full advantage.

As the notion of crime changes, so does the object of crime. The law itself is forced to wrestle with the ambiguous nature of information as property.

With physical objects it is easy to understand the crime of theft, of depriving someone of the possession and use of physical property. With information, the issue is more complex. When a hacker copies a piece of information or even views it without permission, is he or she guilty of theft ? Hackers, by exploiting and exploiting issues of secrecy, question precisely what it is that gives information its value. In doing so, they pose fundamental challenges to the structure of the law and the value and definition of property.

Often seen as computer geniuses or experts, hackers are also positioned in the popular imagination in relation to questions of technological domination. Hackers express, in the most extremes terms, contemporary society’s relationship to ICTs themselves. In doing so, they explore for us issue of technological domination and control45.

45. Supra 8 – P – 15-16.
Concluding Comments:

This Chapter provides an overview of Cyber Crime history, starting with the white hat and hacker ethic and type of Cyber Crimes and elements criteria. The global connectivity of the Internet, makes it easier for criminals to act beyond national boundaries to conduct their illegal affairs. The perpetrators simply capitalize on the weakest links in the system.

This is a new form of crime and has gained very fast recognition demanding attention follow-up and combat. The legislature, judiciary and the law enforcing authorities have to face this new challenge.