CHAPTER 1

INTRODUCTION
A CRIMINOLOGICAL STUDY OF THE IMPORTANCE OF THE
INFORMATION TECHNOLOGY ACT-2000 WITH SPECIAL
REFERENCE TO CYBER CRIMES IN BANGALORE CITY

CHAPTER -1

1. INTRODUCTION

We live in an exciting time of our life. The widespread availability of computers and internet facility provides unprecedented opportunities to communicate with the rest of the world, for trade, commerce and educate ourselves. Although most people use the computer as a powerful and beneficial tool for communication and education, some individuals exploit the power of the computer for criminal or terror purposes.

In the recent days, computers and the internet have entered the into the mainstream of people’s lives. Millions of people spend several hours everyday in front of computers, sending and receiving e-mails, surfing the web, maintain databases, and participate in countless other activities. Unfortunately, those who commit crime have not missed the opportunity out of computer revolution also. An increasing number of criminals use Pagers, Cellular Phones, Laptop Computers and Network Servers in the course of committing various crimes. In some cases, computers provide the means of committing crime. For example, the internet can be used to deliver a death threat via e-mail; to launch hacker attacks against a vulnerable computer network; to disseminate computer viruses; or to transmit images of child pornography. In other cases, computers merely serve as convenient storage devices for evidence of crime. For example, a drug
kingpin might keep a list of who owes him money in a file stored in his desktop computer at home or a money laundering operation might retain false financial records in a file on a network server.

The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers. The capabilities and opportunities provided by the internet have transformed many legitimate business activities, augmenting the speed, ease; and range with which transactions can be conducted while also lowering many of the costs. Criminals have also discovered that the internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the internet involves not only fraud and theft, pervasive pornography and pedophile rings, but also drug trafficking and criminal organizations that are more concerned about exploitation than the kind of disruption that is the focus of the intruder community. In the virtual world, as in the real world, most criminal activities are initiated by individuals or small groups and can best be understood as ‘Disorganized crime’. Yet there is growing evidence that organized crime groups or mafias are exploiting the new opportunities offered by the internet. Organized crime and cyber crime will never be synonymous. Most organized crime will continue to operate in the real world rather than the cyber world and most cyber crime will continue to be the results of individuals rather than criminal organizations. Nevertheless, the degree of overlap between the two phenomena is likely to increase considerably in the next few years.
The growing danger from crimes committed with computer or related information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Self protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced; countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National Governments should examine their current status to determine whether they are sufficient to combat the crimes, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

Effective law enforcement is complicated by the trans-national nature of cyberspace. Mechanisms of operation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.
Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and businesses. Because that extension remains a work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely on secondarily on the deterrence that effective law enforcement can provide.

To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process and technology issues. Organizations need to commit the resources to educate employees on security practices, develop through plans for the handling of sensitive data, records and transaction and incorporate robust security technology, such as firewalls, antivirus software, intrusion detection tools and authentication services throughout the organizations computer system.

These system protection tools, the software and hardware for defending information systems are complex and expensive to operate. To avoid hassles and expense, system manufacturers and system operators routinely leave security features 'turned off', needlessly increasing the vulnerability of the information on the system. Bugs and security holes with known fixes are routinely left uncorrected. Further, no agreed upon standards exist to benchmark the quality of the tools, and no accepted methodology exists for organizations to determine how much investment in security is enough. The inability to quantify the costs and benefits of information security investments leave security managers at disadvantage when competing for organizational resources. Much works remain to improve management and technical solutions for information protection.
1.1: CRIME:

Crime is not a single phenomenon that can be analysed and described in one piece. It is a phenomenon that occurs in every part of the world and at every stratum of the society. The offenders and their victims are of all ages, income levels and backgrounds. A precise definition of crime is by no means an easy task. Cursory analyses of the various definitions of crime are as following:

Sutherland characterizes crime as a symptom of social disorganization.

According to Donald Taft “Crime is a social injury and an expression of subjective opinion varying in time and place.”

Tappan has defined crime as,” an intentional act or omission in violation of the criminal law committed without any defence or justification and penalized by the law as felony or misdemeanor”.

Landis & Landis: “Crime is an act which the state has declared harmful to group welfare and which the state has power to punish”

Sethna M J: Crime may be defined as an act or omission, sinful or non-sinful, which a society or a state has the right to punish or otherwise, deal with under its laws for the time being in force.

1 Dr. Paranjape N.V: “Criminology and Penology” (P.5-6 and 133-141); Central Law Publications, Allahabad, (2007).
Haikerwal: “Form sociological point of view, crime or delinquency implies such behavior of the individual as interfaces with the order of human relationships which society regards as primary conditions for its existence”.

Thomas: Crime is an action which is antagonistic to the solidarity of that group the individual considers his own”.

Elliot and Merrill: “when mans conduct is adjudged antisocial, his behavior differs from accepted behavior, chiefly in the groups definition of the situation”.

Barnes and Teeters: “The term ‘crime’ technically means a form of antisocial behavior that has violated the public sentiment to such an extent as to be forbidden by statutes”.

1.2: HISTORY AND TYPES OF COMPUTERS

Definition of Computer

A computer is a machine that can be programmed to manipulate symbols. Its principal characteristics are:

- It responds to a specific set of instructions in a well-defined manner.
- It can execute a prerecorded list of instructions (a program).
- It can quickly store and retrieve large amounts of data.

Therefore computers can perform complex and repetitive procedures quickly, precisely and reliably. Modern computers are electronic and digital. The actual machinery (wires, transistors, and circuits) is called hardware; the instructions and

---

data are called software. All general-purpose computers require the following hardware components:

- **Central processing unit (CPU):** The heart of the computer, this is the component that actually executes instructions organized in programs ("software") which tell the computer what to do.
- **Memory (fast, expensive, short-term memory):** Enables a computer to store, at least temporarily, data, programs, and intermediate results.
- **Mass storage device (slower, cheaper, long-term memory):** Allows a computer to permanently retain large amounts of data and programs between jobs. Common mass storage devices include disk drives and tape drives.
- **Input device:** Usually a keyboard and mouse, the input device is the conduit through which data and instructions enter a computer.
- **Output device:** A display screen, printer, or other device that lets you see what the computer has accomplished.

In addition to these components, many others make it possible for the basic components to work together efficiently. For example, every computer requires a bus that transmits data from one part of the computer to another.

**Computer sizes and power**

Computers can be generally classified by size and power as follows, though there is considerable overlap:

- **Personal computer:** A small, single-user computer based on a microprocessor.
- **Workstation:** A powerful, single-user computer. A workstation is like a personal computer, but it has a more powerful microprocessor and, in general, a higher-quality monitor.
- **Minicomputer:** A multi-user computer capable of supporting up to hundreds of users simultaneously.
- Mainframe: A powerful multi-user computer capable of supporting many hundreds or thousands of users simultaneously.
- Supercomputer: An extremely fast computer that can perform hundreds of millions of instructions per second.

**Supercomputer and Mainframe**

Supercomputer is a broad term for one of the fastest computers currently available. Supercomputers are very expensive and are employed for specialized applications that require immense amounts of mathematical calculations (number crunching). For example, weather forecasting requires a supercomputer. Other uses of supercomputers scientific simulations, (animated) graphics, fluid dynamic calculations, nuclear energy research, electronic design, and analysis of geological data (e.g. in petrochemical prospecting). Perhaps the best known supercomputer manufacturer is Cray Research.

Mainframe was a term originally referring to the cabinet containing the central processor unit or "main frame" of a room-filling Stone Age batch machine. After the emergence of smaller "minicomputer" designs in the early 1970s, the traditional big iron machines were described as "mainframe computers" and eventually just as mainframes. Nowadays a Mainframe is a very large and expensive computer capable of supporting hundreds, or even thousands, of users simultaneously. The chief difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing a few programs as fast as possible, whereas a mainframe uses its power to execute many programs concurrently. In some ways, mainframes are more powerful than supercomputers because they support more simultaneous programs. But supercomputers can execute a single program faster than a mainframe. The distinction between small mainframes and minicomputers is vague, depending really on how the manufacturer wants to market its machines.
Minicomputer

It is a midsize computer. In the past decade, the distinction between large minicomputers and small mainframes has blurred, however, as has the distinction between small minicomputers and workstations. But in general, a minicomputer is a multiprocessing system capable of supporting from up to 200 users simultaneously.

Workstation

It is a type of computer used for engineering applications (CAD/CAM), desktop publishing, software development, and other types of applications that require a moderate amount of computing power and relatively high quality graphics capabilities. Workstations generally come with a large, high-resolution graphics screen, a large amount of RAM, built-in network support, and a graphical user interface. Most workstations also have a mass storage device such as a disk drive, but a special type of workstation, called a diskless workstation, comes without a disk drive. The most common operating systems for workstations are UNIX and Windows NT. Like personal computers, most workstations are single-user computers. However, workstations are typically linked together to form a local-area network, although they can also be used as stand-alone systems. In networking, workstation refers to any computer connected to a local-area network. It could be a workstation or a personal computer.

Personal computer:

It can be defined as a small, relatively inexpensive computer designed for an individual user. In price, personal computers range anywhere from a few hundred pounds to over five thousand pounds. All are based on the
microprocessor technology that enables manufacturers to put an entire CPU on one chip. Businesses use personal computers for word processing, accounting, desktop publishing, and for running spreadsheet and database management applications. At home, the most popular use for personal computers is for playing games and recently for surfing the Internet.

Personal computers first appeared in the late 1970s. One of the first and most popular personal computers was the Apple II, introduced in 1977 by Apple Computer. During the late 1970s and early 1980s, new models and competing operating systems seemed to appear daily. Then, in 1981, IBM entered the fray with its first personal computer, known as the IBM PC. The IBM PC quickly became the personal computer of choice, and most other personal computer manufacturers fell by the wayside. P.C. is short for personal computer or IBM PC. One of the few companies to survive IBM's onslaught was Apple Computer, which remains a major player in the personal computer marketplace. Other companies adjusted to IBM's dominance by building IBM clones, computers that were internally almost the same as the IBM PC, but that cost less. Because IBM clones used the same microprocessors as IBM PCs, they were capable of running the same software. Over the years, IBM has lost much of its influence in directing the evolution of PCs. Therefore after the release of the first PC by IBM the term PC increasingly came to mean IBM or IBM-compatible personal computers, to the exclusion of other types of personal computers, such as Macintoshes. In recent years, the term PC has become more and more difficult to pin down. In general, though, it applies to any personal computer based on an Intel microprocessor, or on an Intel-compatible microprocessor. For nearly every other component, including the operating system, there are several options, all of which fall under the rubric of PC.

Today, the world of personal computers is basically divided between Apple Macintoshes and PCs. The principal characteristics of personal computers are that they are single-user systems and are based on microprocessors. However, although personal computers are designed as single-user systems, it is common to
link them together to form a network. In terms of power, there is great variety. At the high end, the distinction between personal computers and workstations has faded. High-end models of the Macintosh and PC offer the same computing power and graphics capability as low-end workstations by Sun Microsystems, Hewlett-Packard, and DEC.

**Personal Computer Types**

Actual personal computers can be generally classified by size and chassis/case. The chassis or case is the metal frame that serves as the structural support for electronic components. Every computer system requires at least one chassis to house the circuit boards and wiring. The chassis also contains slots for expansion boards. If you want to insert more boards than there are slots, you will need an expansion chassis, which provides additional slots. There are two basic flavors of chassis designs—desktop models and tower models—but there are many variations on these two basic types. Then come the portable computers that are computers small enough to carry. Portable computers include notebook and sub-notebook computers, hand-held computers, palmtops, and PDAs.

**Tower model**

The term refers to a computer in which the power supply, motherboard, and mass storage devices are stacked on top of each other in a cabinet. This is in contrast to desktop models, in which these components are housed in a more compact box. The main advantage of tower models is that there are fewer space constraints, which makes installation of additional storage devices easier.

**Desktop model**

A computer designed to fit comfortably on top of a desk, typically with the monitor sitting on top of the computer. Desktop model computers are broad and low, whereas tower model computers are narrow and tall. Because of their shape, desktop model computers are generally limited to three internal mass storage
devices. Desktop models designed to be very small are sometimes referred to as **slimline models**.

**Notebook computer**

An extremely lightweight personal computer. Notebook computers typically weigh less than 6 pounds and are small enough to fit easily in a briefcase. Aside from size, the principal difference between a notebook computer and a personal computer is the display screen. Notebook computers use a variety of techniques, known as flat-panel technologies, to produce a lightweight and non-bulky display screen. The quality of notebook display screens varies considerably. In terms of computing power, modern notebook computers are nearly equivalent to personal computers. They have the same CPUs, memory capacity, and disk drives. However, all this power in a small package is expensive. Notebook computers cost about twice as much as equivalent regular-sized computers. Notebook computers come with battery packs that enable you to run them without plugging them in. However, the batteries need to be recharged every few hours.

**Laptop computer**

A small, portable computer -- small enough that it can sit on your lap. Nowadays, laptop computers are more frequently called notebook computers.

**Subnotebook computer**

A portable computer that is slightly lighter and smaller than a full-sized notebook computer. Typically, subnotebook computers have a smaller keyboard and screen, but are otherwise equivalent to notebook computers.

**Hand-held computer**

A portable computer that is small enough to be held in one's hand. Although extremely convenient to carry, handheld computers have not replaced
notebook computers because of their small keyboards and screens. The most popular hand-held computers are those that are specifically designed to provide PIM (personal information manager) functions, such as a calendar and address book. Some manufacturers are trying to solve the small keyboard problem by replacing the keyboard with an electronic pen. However, these pen-based devices rely on handwriting recognition technologies, which are still in their infancy. Hand-held computers are also called PDAs, palmtops and pocket computers.

Palmtop

A small computer that literally fits in your palm. Compared to full-size computers, palmtops are severely limited, but they are practical for certain functions such as phone books and calendars. Palmtops that use a pen rather than a keyboard for input are often called hand-held computers or PDAs. Because of their small size, most palmtop computers do not include disk drives. However, many contain PCMCIA slots in which you can insert disk drives, modems, memory, and other devices. Palmtops are also called PDAs, hand-held computers and pocket computers.

PDA

Short for personal digital assistant, a handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer. Unlike portable computers, most PDAs are pen-based, using a stylus rather than a keyboard for input. This means that they also incorporate handwriting recognition features. Some PDAs can also react to voice input by using voice recognition technologies. The field of PDA was pioneered by Apple Computer, which introduced the Newton MessagePad in 1993. Shortly thereafter, several other manufacturers offered similar products. To date, PDAs have had only modest success in the marketplace, due to their high price tags and limited applications. However, many
experts believe that PDAs will eventually become common gadgets. PDAs are also called palmtops, hand-held computers and pocket computers.

1.3: CYBERSPACE:

The term “Cyberspace”, according to Webopedia is defined as:

(1) A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. Some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. The term was coined by author William Gibson, an U.S. Citizen, in his sci-fi novel Neuromancer (1984).^3

---

1.4: DEFINITIONS OF CYBER CRIME:

The task of defining Cyber Crime is not simple, as several scholars and
governments rarely concur on what a comprehensive definition may be. A few of
the definitions that which have been widely accepted are as following:

Melanie Kowalski in “Cyber-Crime: Issues, Data Sources, and Feasibility of
Collecting Police-Reported Statistics” Published by authority of the Minister
responsible for Statistics Canada defines Cyber crime as “To date, no single
definition of cyber-crime has emerged that the majority of police departments use.
The following working definition has increasingly been accepted by Canadian law
enforcement agencies: “a criminal offence involving a computer as the object of
the crime, or the tool used to commit a material component of the offence.”

Generally speaking, based on the definition created by the Canadian Police
College and by other research sources (Carter: 1995; Davis and Hutchison: 1997),
there are two broad categories of cyber-crime.

The first category is defined where the computer is the tool of the crime. This
category includes crimes that law enforcement has been fighting in the physical
world but now is seeing with increasing frequency on the Internet. Some of these
crimes include child pornography, criminal harassment, fraud, intellectual
property violations and the sale of illegal substances and goods.

The second category is defined where the computer is the object of the
crime. Cyber-crime consists of specific crimes dealing with computers and

4 Melanie Kowalski in “Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported
Statistics” Published by authority of the Minister responsible for Statistics Canada
networks. These are new crimes that are specifically related to computer technology and the Internet. For example, hacking or unauthorized use of computer systems, defacing websites, creation and malicious dissemination of computer viruses.

In addition to cyber-crime, there is also "computer-supported crime" which covers the use of computers by criminals for communication and document or data storage.

The terms "computer crime", "computer-related crime", "high-tech crime", "cyber-crime" and "Internet crime" are often used interchangeably when police and other information sources are discussed.

(This definition is offered at the Canadian Police College, where Canadian police officers undergo training in computer crime investigative techniques.)

According to Barkha Bhasin and U. Rama Mohan "Computer crime can be defined as crime against an organization or an individual in which the perpetrator of the crime uses a computer or any computer enabled technology for all or part of the crime"5

Webopedia definition: "Cyber Crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, Cyber Crime

---

5 Barkha and Rama Mohan; "Cyber Law and Crimes" (P. 7-11); Asia Law House; Hyderabad (2006)
also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be Cyber Crimes when the illegal activities are committed through the use of a computer and the Internet”.

**Techterms definition:** “Cyber Crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber Crime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet”\(^6\).

A simple yet sturdy definition of Cyber Crime would be "unlawful acts wherein the computer is either a tool or a target or both".

**Wikipedia definition:** “Cyber Crime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories”\(^7\).

**United Nations definition of Cyber Crimes:** The United Nations has evolved the definition of Cyber Crimes of its 10\(^{th}\) UN congress on the prevention of crime and treatment of offence, defined thus;

---

\(^6\) [http://www.techterms.cybercrime.com](http://www.techterms.cybercrime.com)

\(^7\) [http://www.cybercrimes.wikipedia.com](http://www.cybercrimes.wikipedia.com)
a) Cyber Crime in a narrow sense (computer crime) any illegal behavior directed by means of electronic operations that target the security of a computer systems and data proceed by them.

b) Cyber Crime in a broad sense (computer related crimes), any illegal behavior committed by means of or in relation to a computer system or network, including such crimes as illegal possession and offering or distributory information by means of a computer system or network.

According to Symantec: The term “Cyber Crime” to offenses ranging from criminal activity against data to content and copy right infringement.

According to Zevar—Geose: Definition is broader, including activities such as fraud, unauthorized access, child pornography and cyber stalking.

According to Tech-republic: Cyber Crime is quickly on the rise and cyber criminals are constantly developing new attacks designed to grow their bank account. Cyber Crime threatens organization of all kinds and it can disrupt upon daily business activity or worse, steal your earned profits.

According to British Police: Cyber Crime includes the use of any computer Network for crime.

---

8 Barkhu and Rama Mohan; “Cyber Law and Crimes” (P.7-11); Asia Law House: Hyderabad (2006)

9 http://www.cybercrime.semantic.eom


11 http://www.britishpolice.uk.org
According to Council of Europe – Any criminal offence committed against or with the help of a computer network.

1.5: CHARACTERISTICS OF CRIME

When a careful examination of the ingredients of any crime is made, seven characteristics emerge. The American criminal law scholar Jerome Hall has developed the theory that a human event, in order to qualify as crime, must meet these seven basic requirements, so do Cyber Crimes:

1. The act requirement
2. The legality requirement:
3. The harm requirement
4. The causation requirement
5. The mens rea requirement
6. The concurrence requirement
7. The punishment requirement

The Act Requirement:

Scholars of law have long agreed that the basic ingredient of every crime is a human act. In this context, what constitutes an “act” is a question that has been

much debated. For instance, a sleepwalker, in a trance, grabs a stone and hurls it, which hits a passerby, with lethal consequence. The law does not consider it to be a willful act; before any human behaviour can qualify as a criminal act, there must be a conscious interaction between mind and body, a physical movement that results from the willful determination or conscious effort from the doer.

Cyber crime, like all conventional crime, bears this feature. Further, the question of failure to act or Omission is also specified in the cyber laws, specifically, when the factor of "due diligence" arises. Failure to prevent a Cyber criminogenic situation is held liable on the services provider, in the Information technology Act, 2000.

**The Legality Requirement:**

This is based on the ancient proposition that only conduct that has been made criminal by law before an act is committed can be a crime. It owes its origin to the Latin maxim *nullum crimen sine lege*, which implies that there is no crime without law. In addition to this, when the law has made some behaviour a crime, the language defining it must be clear enough to be understood.

**The Harm Requirement:**

Every act that has been prohibited by law is a crime, primarily due to the fact that it has harmful effects, and is to be prevented. Harm is the detrimental consequence that is sought to be avoided by law enactment. From a criminological perspective, most crimes are grouped by the harm that each entails.
Offence against person involve harm to an individual, offence against property involve damage to property or loss of its possession. Cyber crimes involve the use of computers or the cyber media to commit a crime, which are harmful to the person's reputation or honour, or cause loss of possession or damage to property.

The Causation Requirement:

Causation requirement is that which requires the doer of the act to cause the harm through his or her own effort. It holds that the crime is not complete unless the doers conduct necessarily caused the harm without interference by somebody else and that is the proximate cause of the act.

Mens Rea:

Every crime, according to tradition, requires mens rea or the 'guilty mind'. It is the preparedness or the criminal bent of mind that is the all important factor in determining crime causation. Mens rea is never seen wanting in any white collar crime, including cyber crimes. The offender is always aware of the wrongfulness of his act and as well as the intention to do the act.

Strict liability is an exception to the mens rea requirement. There is a class of offences for which legislatures or courts require no showing of criminal intent or mens rea. For these offences, the fact that the doer makes an innocent mistake and proceeds in good faith does not affect criminal liability. Such
offences are called strict liability offences. There are a number of laws in India that involve these offences. They involve conduct subject to regulation, conduct that threatens the public welfare as a whole. Typically, these offences are subject to small penalties only. The efficacy of strict liability is in doubt. Vast numbers of persons being found guilty who had no idea of doing something wrong form the largest numbers of instances of the white collar and the cyber criminals. The fact is that it is an accepted form of practice within the trade in which they are involved, despite of being violative of law, which governs the trade, is emphasized here.

The Concurrence Requirement:

This requirement states that every criminal act is to be accompanied by an equally criminal mind. The act and intent must incur in this requirement. The General Exceptions of the Indian Penal Code 1861 amply exemplifies as to the circumstances of the accused not being liable of an offence, though, seemingly he or she may have committed it.

The Punishment requirement:

This is the last but the most significant ingredient of crime. An illegal act, coupled with an evil mind does not make it a crime, unless the law subjects it to punishment. The punishment requirement, more than any of the others, is the differentiating aspect between crime and torts.
1.6: TYPES OF CYBER CRIME:

The meaning of cyber crime may be any crime that is committed by means of the special knowledge or expert use of computer technology; harmful acts committed from or against a computer or network; an unlawful act wherein the computer is either a tool or a target or both. Hence the types of cyber crimes, in the opinion of scholars are as following:

Cyber crime can be categorized as:\(^\text{13}\)

- Software related crimes.
- Data related crimes.
- Physical crimes.
- Internet and other computer related crimes.

SOFTWARE RELATED CRIMES:

A. Unauthorized Access: Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system.

\(^{13}\) Singh, Pramod Kumar; “Law on Cyber Crimes” (P.4-11, 14-16 & 40-63) Book Enclaves: New Delhi. (2007)
B. **Salami Attack:** This attack is used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. Example, a bank employee inserts a program into the bank’s servers that deducts a small amount of money (say a Rs.5 a month) from the account of every customer. No single account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

C. **Logic Bomb:** This is event dependent program. This implies that this program is created to do something only when a certain event (known as a trigger event) occurs, example, some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

D. **Virus/Worm Attack:** Virus is a program that attach themselves to a computer or a file and then circulate it selves to other files and to other computer on a network. They usually affect the data on a computer, either by alerting or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer’s memory.

E. **Trojan Attack:** A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

F. **Intellectual Property Crime:** This includes software piracy, copyright infringement, trademarks, violations etc.
G. **Trap Door:** Malicious manipulations of security bypass logic used by system developers to save extra key strokes and enter specific programs.

H. **Time Bombs:** Logics inserted into programs to execute understand work when desired.

I. **Super Zapping:** A logic similar to trap door but more devastative wherein programs can be changed and malicious logics can be induced.

J. **Wire-Trapping:** The criminals insert unauthorized signals on a communication line or data channel either to jam the computer system or access desired data for authorized usage.

K. **Software Piracy:** Duplicating computer programs in violation of copyright laws.

DATA RELATED CRIMES:

A. **Data Diddling:** This kind of an attack involves alerting the raw data just before it is processed by a computer and then changing it back after the processing is completed.

B. **Data Leakage:** Copying the data on any magnetic or other media for fraudulent or illegal usage or blackmailing.

C. **Data Spying:** Access to big network installations using modems and telecom lines through legitimate password or breaking the password for selling it to a competitor or an enemy country for a price.

D. **Scavenging:** A method of obtaining and re-using information left in or around a computer system after processing. The method ranges from physical examining of
dustbins for discarded copies of computer listing to technical search for residual data.

PHYSICAL CRIMES:

A. **Theft**: Taking away the computer, its peripherals, data, software or accessories from the rightful ownership of someone else without the consent and knowledge of the owner.

B. **Breakage**: Sabotaging computer hardware like monitors, keyboards, pouring liquid, powder etc., over keyboard, electronics inserting pins to short circuit the system, cutting cables wires, blocking air flow, arson, bombing or other similar activities.

C. **Destroying Data, Output or Media**: Physically destroying master files by placing magnets near the media like tapes and floppies or scratching the media using a sharp object or physically bending it, misfile or erase active master files.

D. **Inter-Processing Manipulations**: Tampering with master files between normal processing cycles by getting possession of the new master file and altering one or more records for fraudulent purposes etc.

**Internet and Other Computer Related Crimes:**

A. **E-mail Bombing**: E-mail bombing refers to sending a large amount of e-mails to the victim resulting in the e-mail account (in case of an individual) or mail server (in case of a company or an e-mail service provider) crashing.
B. Internet Time Theft: This connotes the usage by an unauthorized person of the internet hours paid for by another person.

C. Cyber Pornography: Creating websites that cater nude pictures and literatures. This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the internet (to download and transmit pornographic pictures, photos, writings, etc.)

D. E-mail Spoofing: A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source.

E. Cyber Stalking: The oxford dictionary defines stalking as ‘pursuing stealthily’. Cyber stalking involves following a person’s movements across the internet by posting massages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-room frequently by the victim, constantly bombarding the victim with e-mails etc.

F. Password Attacks: Attempts to obtain or identify a user account or password using different methods like Trojan horse, IP spoofing, packet sniffers etc.

G. Brute-Force Attack: A method of implementing a password attack using a program that runs across the network and logs into a shared resources such as a server.


I. Hacking: Unauthorized access to programs, systems etc., with an intention to commit further offences. There are various kinds of hackers like Crackers, Code Hackers, Cyber punks, Phreakers etc.
J. **Blackmailing**: The old crime of blackmailing on the new medium of internet.

K. **Frauds**: Committing frauds through online investment newsletters, bulletin boards, e-mail online spasm etc.

THE INTERNATIONAL POLICE ORGANISATION (INTERPOL)

CLASSIFICATION OF CYBER CRIME:

1. Unauthorised access or interception and theft of data (hacking, etc)
2. Alteration of computer data (logic bomb, Trojan horse, virus, worm, etc)
3. Computer related fraud (A T M, cash dispensers, credit cards, computer forgery, gaming machines, input/output / and program manipulations, telephone phreaking etc)
4. Unauthorised reproductions (software piracy)
5. Computer sabotage (hardware/ software etc)
7. Computer pornography.
8. Computer related crime (BBS, theft of trade secrets etc.)

RESEARCHER’S ATTEMPT TO CLASSIFY CYBER CRIMES:

The subject of cyber crime may be broadly classified under the following three groups.

---

14 Barkha and Rama Mohan; "Cyber Law and Crimes" (P.7-11); Asia Law House; Hyderabad (2006)
A. Against Individuals:

a. Their person and;

b. The property of an individual.

B. Against Organization:

a. Government;

b. Firm, Company, Group of Individuals.

C. Against Society at large

The following are the crimes, which can be committed against the followings group

Against Individuals: –

i. Harassment via e-mails.

ii. Cyber-stalking.

iii. Dissemination of obscene material.

iv. Defamation.

v. Unauthorized control/access over computer system.

vi. Indecent exposure
vii. Email spoofing

viii. Cheating & Fraud

Against Individual Property:

i. Computer vandalism.

ii. Transmitting virus.

iii. Netrespass

iv. Unauthorized control/access over computer system.

v. Intellectual Property crimes

vi. Internet time thefts

Against Organization:

i. Unauthorized control/access over computer system

ii. Possession of unauthorized information.

iii. Cyber terrorism against the government organization.

iv. Distribution of pirated software etc.

Against Society at large:

i. Pornography (basically child pornography).

ii. Polluting the youth through indecent exposure.
The above mentioned offences may discussed in brief as follows:

1. **Harassment via e-mails-**

   Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Harassment may be in the form of blackmail, threaten to expose her etc.

2. **Cyber-stalking-**

   The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

3. **Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) / Polluting through indecent exposure-**

   Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing
these obscene materials. Downloading through the Internet, obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

4. **Defamation**

It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.

4. **Unauthorized control/access over computer system**-

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

5. **E mail spoofing**-

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates

6. **Computer vandalism**-
Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

7. **Transmitting virus/worms**-

Intentionally disseminating virus or worm into another’s system; to introduce Malware intentionally.

8. **Intellectual Property crimes / Distribution of pirated software**-

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.

9. **Cyber terrorism against the government organization**

At this juncture a necessity may be felt that what is the need to distinguish between cyber terrorism and cyber crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime is generally a domestic issue, which may have international consequences, however cyber terrorism is a global concern, which has domestic as well as international
consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc.

Cyber terrorism may be defined to be “the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives”

A cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

10. Trafficking

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.

11. Fraud and Cheating

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the
cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

In spite of the types of regular crimes listed down by various national and international law enforcement bodies, new and spectacular crimes take birth with the passage of time. One can hardly imagine the variety and diversity of the types of crimes committed with or against the information systems. Crime per say may be old but the medium may be ingeniously new. Computer crimes are also different from other conventional crimes in its way of easy commission and difficulty in detection. Still harder is the task of proving it. All these intricate networks of modus operandi used by the criminals in addition to the technical labyrinth calls for sophisticated systems and highly skilled individuals to detect and investigate computer crimes.

1.7: DISTINCTION BETWEEN CONVENTIONAL AND CYBER CRIME-

Upon a broader inspection, there is no distinction apparent between cyber crimes and conventional crimes. A closer look indicates that there exists a very fine demarcation between the two. The demarcation lies in the involvement of the medium in cases of cyber crime. The *sine qua non* for cyber crime is that there should be an involvement, at any stage, of the virtual cyber medium. Cyber crimes, like conventional crimes have all the characteristics of crime.
To contrast traditional criminal activity cyber-criminal activity is not as simple as it is superficially seen. Broadly speaking, traditional criminal activity displays some fairly characteristic and commonly understood features (Braithwaite, 1992; Gottfredson & Hirschi, 1990).

First, there is a degree of consensual or core values within a society as to what does and does not constitute a crime, and these shared values are usually based in criminal law.

Second, criminal activities tend to take place in real time because their time frame is largely determined by the physical world, for example, having to take account of the speed of transport, the physical size of the haul, and the needs of the offenders involved.

Third, the majority of offending and victimization tends to take place within a distinct geographic boundary.

Fourth, the criminology of traditional crime tends to be offender based rather than victim or offense based.

Fifth, serious fraud incidents notwithstanding, much of the debate over traditional crime has tended to focus on Working-class subcultures. In contrast, cybercrimes would appear to exhibit nearly the opposite characteristics. They are contentious in that there does not yet exist a core set of values about them. They appear to be largely free of a physical time frame; therefore, they are relatively, if not totally, instantaneous. Cybercrimes can also be transnational, trans-jurisdictional, and global, and if there is topography of the Internet, it is expressed more in terms of levels of access to the Internet and language rather than in terms
of physical geography. The discussion of cyber crimes has tended to be offense based rather than victim or offender based.

Finally, Cybercrimes tend to cover a broad range of legal issues, many of which are the subject of civil law in addition to, or instead of, criminal law, demonstrating a resonance with the study of white-collar crime. It is the traditional model of crime, however, that tends to underpin the criminal justice paradigm and, therefore, informs our understanding, thereby highlighting the need to explore the maintenance of order and law on the Internet. Incidentally, the terms order and law are deliberately reversed here and elsewhere to break the conceptual link that has increasingly bound the two concepts since the late 1970s (see also Fowles, 1983, p. 116; Wall, 2001, p. 167).

1.8: REASONS BEHIND CYBER CRIME

There are various reasons for committing cyber crimes. Some of the reasons are, such as:

Hart in his work “The Concept of Law” has said ‘human beings are vulnerable so rule of law is required to protect them’. Applying this to the cyberspace we may say that computers are vulnerable. So rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

A. Capacity to store data in comparatively small space-
The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much more easier.

B. Easy to access-

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

C. Complex-

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

D. Negligence-

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there
might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

E. Loss of evidence-

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

F. Pecuniary-

Finance is the means for many of the crimes and cyber crime is not far from it. Indeed all the four dark horses of modern civilization – money laundering, drugs, terrorism and child pornography – are available in the cyberspace and have benefited immensely from activities in the cyberspace. To succeed in the cyberspace, all that the perpetrators of these crimes have to do is to hire and nurture intelligent computer literates, hackers and cyber scoundrels to aid their cause.

G. Social status-

People tend to be in the higher status in the society. While some try to improve their social status by dint of hard work, others try it the criminal way and as a result they may try on computers too. The desire for status and the ambition leads the professionals to cyber crimes.

H. Terrorism-
Terrorists are known to use Information Technology and the Internet to formulate plans, raise funds, spread propaganda and to communicate security. For example, convicted terrorist, Ramzi Yousif, the mastermind of the World Trade Center bombing, stored detailed plans to destroy US airlines, on encrypted files on his laptop computer. Moreover, some groups have already used cyber attacks to inflict damage on their enemies’ information systems. For example, a group calling itself the Internet Black Tigers conducted a successful ‘denial of service’ attack on servers of Sri Lankan government embassies.

I. Curiosity-

Curiosity is one of the main force which drives mankind to inventions and discoveries. And these discoveries are sometimes immensely beneficial and sometimes terribly destructive to us. Some people are quite curious by nature. They have a natural flair for research and development and as a consequence try to understand and experiment every thing occupying their interest, sometimes producing some highly unwanted discoveries. The same is true for computer professionals, bugs and viruses are results of curious minds.

J. Psychological Factors

The rapid growth of technology has produced equally rapid growth of ‘technostress’ Amongst the users of technology. The same is true for
computer users. During stress, if a person loses control over himself and which may lead for computer crime or to anything. Frustration and depression too cause a high crime toll in computers. Also a person who is sick mind, who thinks negatively, can harm or commit a computer crime.

K. Revenge

Sometimes, computer crimes are committed, as generously a revenge of a person against the owner or the user of the computer system. Most of the computer crimes for revenge are committed by ex-employees. In these cases the person is in possession of adequate knowledge and information as to how he should go about his way in seeking the revenge, as he had worked with the establishment.

1.9: CYBER CRIMINALS:

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals-

1. Children and adolescents between the age group of 6 – 18 years –

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding
Amongst other children in their group. Further the reasons may be psychological even. E.g. the *Bal Bharati* (Delhi) case was the outcome of harassment of the delinquent by his friends.

2. Organised hackers-

These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the *NASA* as well as the *Microsoft* sites is always under attack by the hackers.

3. Professional hackers / crackers –

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

4. Discontented employees-

This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.
1.10: ‘MODUS OPERANDI’ OF CYBER CRIME:

A. Unauthorized access to computer systems or networks / Hacking-

This kind of offence is normally referred as hacking in the generic sense. However the framers of the information technology act 2000 have no where used this term so to avoid any confusion we would not interchangeably use the word hacking for ‘unauthorized access’ as the latter has wide connotation.

B. Theft of information contained in electronic form-

This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

C. Email bombing-

This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

D. Data diddling-

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed.
E. Salami attacks-

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein, a disgruntled employee, working as a computer programmer upon being dismissed from service programmed a code, called as a logic bomb, was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

F. Denial of Service attack-

The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (D DoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

G. Virus / worm attacks-

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10
million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. It almost brought development of Internet to a complete halt.

H. Logic bombs-

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

I. Trojan attacks-

This term has its origin in the word ‘Trojan horse’. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail.

J. Internet time thefts-

Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password.

K. Web jacking-
This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money.

1.11: ORGANISATION OF THE STUDY

The entire study is organised in five different chapters.

Chapter-1: Introduction-

This chapter includes the introduction to the research topic, meaning and historical development of Computers, characteristics of crime, cyber crime, types of cyber crimes and the problems relating to it.

Chapter-2: Review of Literature and Theoretical Framework.

Chapter-3 Research Methodology-

The contents of this chapter are Aims, Objectives, Hypothesis, Statement of the problem, Area, Scope, Sampling, Tools and Techniques and as well as the Limitations of the Study.

Chapter-4: Data Analysis and Interpretation-
This chapter deals with the analysis of the tabulated data, which is supported with the help of interpretation of each Table, which aid in arriving at appropriate results.

Chapter-5: Findings, Suggestions and Conclusion-

This chapter consists the three important aspects of study; Findings, Suggestions and Conclusions. Based on the Findings of the Study, Suggestions are made and Conclusions are drawn. This is followed by the Bibliography.

Maps, Graphs and photographs along with citations from books and journals are used at appropriate places.