CHAPTER-III
MEANING, CONCEPT AND CLASSIFICATION
OF CYBER CRIMES

3.1. Introduction

“It is very essential to emphasis here that the world it not run by weapons any more,
or energy, or money. It is run by ones and zeros …. little bits of data …. It is all
electrons. There’s a war out there, a world war. It’s not about who has the most
bullets. It is about who controls the information – what we see and hear, how we
work, what we think. It’s all about information” The movie traced on Information
Technology to commit theft in superhighway and information is the commodity to
theft.¹

From the start of the new millennium, social networking sites have become very
popular. These sites have provided a space for many to vent their feelings, get new
and connect with old friends.² But these sites have been misused by cyber criminal
groups unfortunately for fulfilling their illegal purposes. Side by side the people have
started to spend more and more time on such networks over the last few years because
the peoples increasingly rely on them. In the modern time period the development of
Information Technology effects the life of the people’s all around the world. New
inventions and discoveries day-by-day has widen the scientific scope as well as
brought the new challenges for legal world. With the widespread growth of these
technology leads to commission of new types of crimes today on the cyber space and
also has become matter of global concern in future.

In the era of cyber world as the usage of computers became more popular, there was
expansion in the growth of technology as well, and the term ‘Cyber’ became more
familiar to the people. The evolution of Information Technology (IT) gave birth to the
cyber space wherein internet provides equal opportunities to all the people to access

² David Decary Hetu and Carlo Morselli, “Gang Presence in Social Network Sites”, International
any information, data storage, analyse etc. with the use of high technology. These crimes are as like the attack on the secured information of individuals, corporations, or governments. These types of attacks do not take place on a physical body but on the personal or corporate virtual body.

Over the past two decades, technology has surged into businesses, communities, and the lives of individuals, altering the way that people communicate, study, work, and interact. People in various parts of the world can communicate in real time on a variety of devices such as cell phones, tablets or computers. In a few seconds, a photo, video, text message, or email which is shared by a single individual may be viewed by hundreds or thousands of users and may go viral. The Internet technology has also become a new medium for doing misconduct or to threaten, harass, intimidate and cause harm to others.

From a socio-cultural perspective, there is a detrimental separation between the social (norms, legislation) and environmental (computer availability) constraints of computer criminal behavior, which is a direct result of the globalization of technology. Despite such a great influence of computers and internet on day-to-day lives, the fact remains that only a fraction of people know what computer and internet is all about? There is a need of systematic study which elaborately discusses the basic concepts of crime, cyber crime, cyber space and meaning, types, characteristics and major components of cyber crime etc.

### 3.2. Concept of Cyberspace

The term ‘cyber space’ was first used by William Gibson, which he later described as ‘an evocative and essentially meaningless’ buzzword that could serve as a cipher (transforming a text in order to conceal its meaning) for all of his cybernetic thoughts.

---

Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. The virtual space in which all of Information Technology mediated communication and actions are taking place is often referred to as ‘Cyber Space’. Cyberspace cannot be spatially located. It is made up of intangible objects, such as your website, blog, social networks, email accounts, personal information and reputation. Cyber space can be thought of as a global electronic village with instantaneous communication and no geographical barriers.

Cyberspace is the electronic medium of computer networks, in which online communication takes place and where individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games engage in political discussions etc. Cyberspace the new frontier, is the common heritage of mankind but unfortunately some people misuse the common heritage and therefore, cyberspace is also a new frontier of different type of crimes.

Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. The persons involved in cyberspace are known as netizens which comes from the association of two words ‘Internet’ and ‘citizen’. Thus Netizens means any person who is associated with the use of computers, information technology and the Internet.

According to Webster’s Dictionary, Cyberspace is the electronic system of interlinked networks of computers, bulletin boards, etc. that is thought of as being a boundless environment providing access to information, interactive communication, and, in science fiction, a form of virtual reality. Cyberspace means that ‘the notional environment in which electronic communication occurs or virtual reality’.

According to Chip Morningstar and F. Randall Farmer, cyberspace is defined more by social interactions involved rather than its technical implementation. The core

---

9 _Supra_ note 7.
11 _Supra_ note 7.
characteristic is that must be an environment which consists of many participants with the ability to affect and influence each other. In cyberspace, the computational medium is an augmentation of the communication channel between real people.\textsuperscript{14}

### 3.3. Concept of Crime

As truly said, crimes have “.....always depended on the force, vigour and movement of public opinion from time to time and country to country and even in the same country, from decade to decade”.\textsuperscript{15} Crime is timeless, it has been here since society began and will be here forever. As long as society improves its safeguards, criminals will change their approaches.\textsuperscript{16} To understand the concept of crime, an attempt has been made to explain it from the very early time period to modern concept of crime. These two time periods are explained as under:

#### 3.3.1. Early Concept of Crime

Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crime depending on their nature and extent.\textsuperscript{17} Historically, the English society prior to 10\textsuperscript{th} century confused crimes with torts because the bond of family was far stronger than that of the community, the injured party and his kindred could avenge the wrong by private vengeance and self-redress and recourse to legal remedy was considered merely an optional alternative to self-redress.\textsuperscript{18}

At that time the wrongdoer was supposed to offer compensation to the suffered person and the quantum of compensation was based on the extent of the wrong caused and the status of the suffered person in the society. We can say that as compare to modern time, the law did not compel in early days for regulating the social relations. During the 12\textsuperscript{th} and 13\textsuperscript{th} centuries the Early English society included only those acts as crimes

\textsuperscript{14} Available at: http://en.wikipedia.org/wiki/Cyberspace#cite_note-3 (visited on June 6, 2016).
\textsuperscript{18} Amita Verma, Cyber Crimes & Law, 2009, p. 34.
if committed against the state or the religion not others. There was no recognition of distinction between the law of crime and torts during the early societies and these societies only follow the law of wrongs. After entering into the modern legal systems the law is administered at once irrespective of the wants of the suffered party as soon as an offence is committed but in early societies the law was set into motion only when both the parties wants to submit themselves to the judgement. During the period of 18th century also called as an era of miraculous reorientation in criminology, it was believed that only the wrongdoer himself could admit his criminal responsibility for his crime and no one including any external agencies had anything to do with it. At that time it was clear that the concept of crime is interlinked with social policy of that time.

In the ancient society, where many facets of human life like agriculture, political institutions, health services, medical science and basic amenities of life were at a rudimentary stage, crime too were fewer in number and whenever occurred, they were simple in nature and percolated from baser human instincts like lust, greed, vengeance, jealousy and sexual drive. It was also said that traditionally, crimes were also committed on the basis of physical force, body muscles, and threatening instruments.

The incidence of crime in western countries is far greater than that of India perhaps, because of the variance of social conditions in these countries. The growth rate of crime is increasing due to modernization, urbanization, industrialization, advance of science and technology and civilization. The Scientist well knows the method that how to find out those criminals who are involved in carrying out their criminal activities and also avoid their detection because the risk involved in committing crimes is also lesser. After this there was the greater need for a new approach to crime and criminals so as to combat with the new situations and criminals.

3.3.2. Modern Concept of Crime

Modern approach to crime is a functional approach. Scientific development, industrial revolution, refinement of political institutions, education and academic
enlightenment of the individual, the loosening of religious grip over society and the fading moral norms have changed the configurations of crime in modern society more so in the information society.\textsuperscript{22}

The law is vary in character, so forever changing, adding new crimes to the catalogues and modifying, altering and repealing former ones. There have been astonishing changes in the area of crime.\textsuperscript{23} All over the world the changing concept of crime is depend upon the evolution of the human beings in society. In different countries the concept of crime appears in different lights at different time because a crime in one country may not be a crime in another and a crime at one time may not be a crime at another and vice versa.

The rise of the modern method of criminality due to economic development and the concentration of wealth, rapid improvement in mass media have also changed the concept of traditional crimes like murder, dacoity, robbery, burglary, theft, prostitution, rape, etc. both qualitatively and quantitatively and have given to new forms of crimes.

Crime wave is now measured in hours and minutes rather than in months and years.\textsuperscript{24} Its growth can also be attributed to all the social and economic reasons but it has additional reasons for its unabated growth i.e. its ability to provide a reasonable anonymity to the criminal and irrelevance of geographical borders making jurisdiction completely impossible to define and giving a fair chance to criminal to escape legal action, which in turn encourages them to go further. Therefore, concept of cybercrime finds its explanation in all those in other crimes with additional features of its vastness, anonymity and lack of legal control regimes.\textsuperscript{25}

3.4. Nature of Crimes

Generally speaking, almost all societies have certain norms, beliefs, customs and traditions which are implicitly accepted by its members as conducive to their well being and healthy development. Infringement of these cherished norms and customs is

\textsuperscript{22} Supra note 19, p. 62.
\textsuperscript{23} Supra note 18, p. 36.
\textsuperscript{25} Supra note 18, pp. 36-37.
condemned as anti-social behaviour.\textsuperscript{26} Human conducts which are prohibited by Criminal Law and for which State imposes punishment through Criminal Law are to be treated as crimes. There are several human conducts in our society some are prohibited by moral code i.e. immoral, some are prohibited by civil law i.e., civil wrong and some are prohibited by criminal law i.e., crimes and those which are not prohibited by any of these are not wrong. Therefore, crime is criminal wrong.\textsuperscript{27} The changing nature of the crime can be understood by the following way:

Crime can be understood as Public wrong. According to Blackstone crime is a public wrong. He defines crime in two ways: firstly, crime is an act committed or omitted in violation of a public law forbidding or commanding it. This definition we cannot accept in its entirety because Constitutional Law, Administrative Law etc. are Public Law violations of which are not crimes. Secondly, he modifies his definition and says that a crime is a violation of the public right duties due to the whole community, considered as a community.\textsuperscript{28}

Stephen, the editor of Blackstone’s Commentaries further modified the above definition and said ‘a crime is a violation of a right, considered in reference to the evil tendency of such violation as regards the community at large’.\textsuperscript{29} Thus both, Blackstone and Stephen stress that crimes are breaches of ‘those laws which injure the community’. Stephen further added that ‘crime is an act which is both forbidden by law and revolting to the moral sentiments of the society.’\textsuperscript{30}

In the second way, Crime can be understood as Social wrong. John Gillin defines crime as an act that has been shown to be actually harmful to society, or that is believed to be socially harmful by a group of people that has the power to enforce its beliefs, and that places such act under the ban of positive penalties.\textsuperscript{31} Raffeale Garafalo says crime is an immoral and harmful act that is regarded criminal by public opinion because it is an injury to so much of the moral sense as is represented by one

\textsuperscript{26} N.V. Paranjape, \textit{Criminology and Penology}, 2009, p. 5.
\textsuperscript{27} \textit{Supra} note 1, p. 6.
\textsuperscript{30} \textit{Supra} note 26, p. 6.
or the other, of the elementary altruistic sentiments of probity and pity (honesty). Moreover, the injury must be to these sentiments not in their superior and finer degrees, but in the average measure in which they are possessed by a community as measure which is indispensable for the adaptation of the individual to society.\footnote{K.N. Pillai, Principles of Criminology, 1920, p. 6.}

Supporting this contention Sutherland characterises crime as a symptom of social disorganization. The tendency of modern sociological penologists is, therefore, to treat it as a social phenomenon which receives disapprobation of the society.\footnote{Supra note 30.}

In the third way, Crime can be understood as Conventional wrong. Edwin Sutherland defines crime as criminal behaviour in violation of the criminal law. No matter what the degree of immorality, reprehensibility of indecency of an act, it is not a crime unless it is prohibited by the criminal law. The criminal law, in turn, is defined conventionally as a body of specific rules regarding human conduct which have been promulgated by political authority, which apply uniformly to all members of the classes to which the rules refer, and which are enforced by punishment administered by the State. The characteristics which distinguish this body of rules regarding human conduct from other rules are therefore, polytonality, specificity, uniformity and penal sanction.\footnote{Edwin. H. Sutherland., Principles of Criminology, 1965, p. 4.}

In the fourth way, Crime can be understood as procedural wrong. Austin says a wrong which is pursued by the sovereign or his subordinate is a crime. A wrong which is pursued at the discretion of the injured party and his representatives is a civil injury.\footnote{Austin, Lecture on Jurisprudence, 1920, pp. 249-253.}

Kenny modified Austin’s definition that crimes are wrongs, whose sanction is punitive and is in no way remissible by any private person, but is remissible by the crown alone, if remissible at all.\footnote{Supra note 29.}

Fifthly, Crime can be understood as Legal wrong. Halsbury defines crime as an unlawful act which is an offence against the public and the perpetrator of that act is liable to legal punishment.\footnote{Supra note 26, pp.6-7.} According to criminal law any conduct of human being which is prohibited by law is considered as crime but not included all the conduct of
human being. That’s why it can be understood as legal wrong. Section 40 of the Indian Penal Code defines the term offence as a thing which is made punishable by this code. In India, penal law prohibits and punish all the wrongful act or conduct or omission which is against the law and against the public policy.

3.5. Fundamental Elements of Crime

In order to prove someone guilty of crime with the exception of Strict Liability crimes, the state must show evidence of both actus reus and mens rea. In olden days in Europe, during the period of strict liability, severe punishments were inflicted upon the wrongdoer in order to placate the outraged deity. Later, the linking of human behaviour with the harm done replaced the divine link with the harm caused and such responsibility extended even to animals and inanimate objects like carts, cauldrons, baulks of timber, wheels, boats and the like. Before inflicting some punishments, not only the actus reus, but also the mens rea with which the actus reus is done must be proved beyond doubt.

At such a period of time, criminal law was plain and crimes were also simple and limited in nature. But by the onslaught of 13th century, serious offences called felonies came to be recognised and the practice of bot and wit were considered insufficient to punish the guilty. This led to the first distinction between crime and tort. Moral blame was linked with criminal liability. This change in legal thought was recognition of mental element in liability. The two necessary elements of crime are given as under:

5.1 Actus reus in Cyber Crimes

The word actus connotes a ‘mental or spiritual act’. Actus reus may be defined as “such result of human conduct as the law seeks to prevent”. The actus reus of cyber crime is very dynamic and varied. In simple terms, it means a physical result of human conduct and includes all the elements except the mental element. It does not

---

38 Supra note 4, p.162.
39 Supra note 19, p.63.
40 Supra note 19, p.64.
41 Available at: https://www.merriam-webster.com/dictionary/actus (visited on April 9, 2017).
only mean an act but also includes the state of affairs.

J.C. Smith and B. Hogan considered actus reus as such result of human conduct as the law seeks to prevent.\textsuperscript{44} Merely guilty intention is not enough to fix the criminal liability but some act or omission on the part of doer is necessary to complete offence.\textsuperscript{45} Actus reus in cyber crimes has become a challenge as the entire act is committed in intangible surroundings. The perpetrator may leave some footmarks in the machine itself though it becomes a herculean task to prove it in the law courts as, it is required to be in physical form or at least in such a form where it becomes admissible in evidence\textsuperscript{46}.

The element of actus reus in internet crimes is relatively easy to identify, but is very difficult to prove. The fact of the occurrence of the act that can be termed as a crime can be said to have taken place when a person is making use of computer function; or accessing data stored on a computer or from a computer which has access to data stored outside; or attempt to gain access through internet or passes signals through various computers.\textsuperscript{47} In rape cases, the absence of consent on the part of the prosecutrix is an essential constituent of the actus reus. If this absence of consent is not proved by the prosecution then actus reus of the accused will also not prove and here the prosecution will fail. In this sense we can say sometimes mens rea is also the part of actus reus.\textsuperscript{48}

3.5.2 Mens rea in Cyber Crimes

“The jurisprudence of today knows that no crime can be committed unless there is a mens rea.”\textsuperscript{49} Mens rea is the second essential element, which constitutes crime and is often called ‘a guilty mind’. This interpretation underwent a gradual change until modern criminal law came to regard a guilty mind of some kind or some other such mental element as always being necessary.\textsuperscript{50} Mens rea, “guilty mind”, refers to the

\begin{footnotesize}
\begin{itemize}
\item \textit{Supra} note 19, pp.64-65.
\item Pretty Lather, “Cyber Crimes in India and the Legal Regime to Combat”, A Dissertation submitted to University of Delhi, 2006, p. 15.
\item C. Gringras, \textit{The Laws of Internet}, 1997, p. 216.
\item \textit{Supra} note 44.
\item \textit{Supra} note 15, p. 6.
\item \textit{Supra} note 44, p.55.
\end{itemize}
\end{footnotesize}
mal intent of the individual who committed the act.\textsuperscript{51} The act remains the same while the state of mind makes the act ‘reus’ and hence an offence. Almost all crimes require proof of a mental element of some sort. Some courts have held that ‘all crime exists primarily in the mind’. Every offence require a particular state of mind expressed in the particular provision of the law by the words: ‘with intent’, ‘recklessly’, ‘unlawfully’, ‘maliciously’, ‘wilfully’, ‘knowingly’, ‘fraudulently’, ‘knowing or believing’, ‘dishonestly’, ‘corruptly’, ‘allowing’ and ‘permitting’ expressing various states of mind which are different from each other. However, intention, recklessness and knowledge are the fundamental tenets of criminal liability.\textsuperscript{52}

It is consisted of large amount of different mental behaviours like intention, recklessness and negligence etc. Intention word is used for the state of mind of a man for not only his ability to foresee but also includes the will of the possible result of his conduct because it is rightly said that there cannot be intention unless there is foresight. If a man want to do a particular act, so he must have reasonable foresight of the result of such act. Under the Common Law, there is no criminal liability for any loss or harm caused by a person without any intention or any conduct which is not unforeseen.

\textit{Mens rea} has come to be recognised as an essential element of crime except in statutory offences where liability is strict. With the advent of e-crimes, the legal world faces the difficulty, besides many others to pinpoint \textit{mens rea} in cyber crimes.\textsuperscript{53} As essential ingredient for determining \textit{mens rea} in internet crime, on the part of the offender is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized. There must be, on the part of the hacker, intention to secure access, though this intention can be directed at any computer and not at a particular computer. Thus, the hackers need not be aware of which computer exactly he or she was attacking.\textsuperscript{54} There are the two essential ingredients which form the \textit{mens rea} in case of hacking, firstly, the access intended to be secured must have been unauthorized and secondly, as regarding the access there should be awareness on the part of the hacker.

\begin{flushright}
\textsuperscript{51} Supra note 4, p. 162. \\
\textsuperscript{52} Supra note 19, pp. 65-66. \\
\textsuperscript{53} Supra note 19, p. 67. \\
\textsuperscript{54} Supra note 18, p.40.
\end{flushright}
The *mens rea* in case of cyber crimes comprises two essential elements. First, there must be ‘intent to secure access to any programme or data held in any computer, computer system or computer network. Secondly, the person must know at the time that he commits the *actus reus* that the access he intends to secure is unauthorised.\(^5^5\)

The nature of cyber crimes and the skills involved are such that existing legal framework cannot do much to control and contain the same. In fact, the cyberspace technology has undermined to a major extent the traditional legal concepts like property and has impacted the rules of evidence like burden of proof, *locus standi* and concepts of ‘*mens rea*’.\(^5^6\)

### 3.5.3 Criminal Liability in Cyber Crimes

The concept and nature of crime has clearly stated that there are two elements of crime one is *mens rea* and another is *actus reus*. Only *actus reus* is sufficient to impose criminal liability in the crime against State like false evidence, counterfeiting coin, white collar crime, etc. Under the criminal law it is the general principle that a person cannot be convicted of a crime unless it is proved beyond reasonable doubt by the prosecution and his act or omission is prohibited by the criminal law. The person is liable for the same if he had a defined state of mind in relation to the crime committed. It is also considered that an *actus reus* without *mens rea* is not a crime and vice versa.

In case of cyber crime it is very difficult to prove both elements of Crime. *Actus reus* of cyber crime is very dynamic and varied.\(^5^7\) For example, when a person start functioning with computer by the help of a keyboard and mouse and trying to access information on others computer without his consent then there is the existence of *actus reus* in cyber space which the law wants to control.

Cybercrimes have set in a debate as to whether a new legislation is needed to deal with this new form of criminality. There is a school of thought that believes that cybercrimes are not in any way dissimilar to the ordinary crimes like trespass, larceny or conspiracy with a difference that a computer has been used as medium or

---


\(^5^6\) *Supra* note 10, pp.41-42.

\(^5^7\) *Supra* note 1, p.11.
instrument for commission of crime.\textsuperscript{58} The order school give much credence to unique nature of the emerging technologies and unique set of challenges, unknown to the existing criminal jurisprudence; such as nature and scope of cybercrimes, intent and difficulty in locating the offender, jurisdiction and enforcement. It contends that a new comprehensive legislation is needed to deal with cybercrimes.\textsuperscript{59} To control the cybercrimes two strategies can be adopted firstly, computer crime must be approached as both as traditional crime and modern crimes committed through using high tech computers and secondly, computer crime must be approached as a crime which is unique by nature for which new legal framework is required.

3.6. Theories of Criminal Behaviour in Cyberspace

There are various theories of several criminologists on cyber crime who have attempted to understand criminal behavior in cyber space by examining the causes for which criminals are involved in delinquent behaviour in cyberspace and also they have approached to develop effective legal principles for the prevention and control of these type deviant behaviours of cyber criminals.

For this, there are three main branches of criminal science, firstly, Criminology is the main branch of criminal science which deals with causes of crime and also deals whether an atomic structure, social surrounding circumstances or genetic history; which are the contributory factor for crime commission. Secondly, Penology is the other branch of criminal science which deals with theories of punishment, whether preventive theory, rehabilitative theory, deterrent theory, reformative theory, treatment and correction theory which will be proper contemporary social scenario to reduce crime rate. Thirdly, Criminal law is the last branch of criminal science which is the substantive law and defines crimes and prescribes punishments e.g., the Indian Penal Code 1860 for the commission of wrongful act which are prohibited by law and against the public policy. The various theories of criminal behaviour in cyberspace are explained as under:

3.6.1 Differential Association Theory

This theory is based on the principle that contemporary society contains numerous conflicting structures of norms and behaviours as described by Edwin Sutherland in


his book ‘Principles of Criminology’ in the year 1947. This theory mainly deals with the conflicting definitions of appropriate behaviour which are the contributory factor of several crimes. People through communication with other learn certain behaviour those may be criminal or sober. When they learn criminal behaviour from their intimate groups through communication they generally use the same and in this way commit similar crimes. 60 According to this theory individuals mainly learn through interaction with others the values, attitudes, techniques and motives for criminal behaviour. This theory is mainly discussed about the theories of deviance and also focuses on how they learn to become criminals.

In the contemporary time period there are so many hi-tech society and now-a-days it very common to see cyber criminal groups. In the year 1993, it was rightly said by R. Blackburn that the behaviours of an individual is influenced by peer pressures and peer attitudes. In the year 1989, the same was accepted by C. Hollin in his work ‘Psychology and Crime: An Introduction to Criminological Psychology’ in which he says that persons being associated with the criminals have to be criminal and that they only have to express the favourable situation for committing crime.

3.6.2 Social Learning and Bonding Theory

Social learning theory expounds upon Edwin Sutherland’s Differential Association Theory which puts forth that criminal behaviour is learned through close contact with others that behave in a criminal manner. According to social learning theory, cyber criminals learn how to commit their crimes from other people through imitation initially, and then reinforcement of the behaviour by those individuals.61 This theory is also associated with the work of imitation of Prof. Albert Bandura.

Social Bonding Theory is propounded by Hirschi who mainly focuses on the influences that prevent an individual from engaging in criminal activities. It explains an individual's disinclination to commit crime based on their levels of attachment, commitment, and involvement, as well as their beliefs. Unfortunately, in some parts of the world, cybercrime is becoming acceptable as a form of employment rather than

60 Edwin Sutherland, Principles of Criminology, 1947, pp. 82-85.
as a crime because of the allure of quick riches provided to the perpetrators. According to Rational choice theory which is based on a simple cost-benefit analysis that the people himself make the basic decisions whether they can commit a crime or not to commit. This depends on their own will not any other things.

3.6.3 Space Transition Theory of Cyber Crimes

This theory is developed by Jaishankar Kumar in order to explain the causation of crimes in the cyberspace. Cyberspace presents an exciting new frontier for criminologists. Virtual reality and computer mediated communications challenge the traditional discourse of criminology, introducing new forms of deviance, crime, and social control. Some researchers have tried to explain cyber crimes with traditional theories, such as Social Learning Theory, Kohlberg’s Moral Development Theory and Differential Reinforcement Theory, Cohen’s Strain Theory, Deindividuation Theory, Gottfredson and Hirschi’s General Theory of Crime, Routine Activities Theory and multiple theories. This theory tries to explain the nature of behavior of the criminals on the cyber space as well as physical space. According to this theory people behave differently when there is a movement from one space i.e. physical space to another i.e. cyber space and vice versa.

The main postulates of the theory are:

- Persons would not be able to commit a crime in physical space because of their status and position but with their repressed criminal behavior they have a propensity to commit crime in cyberspace
- There are various factors present on the cyberspace which provides the offenders the choice to commit cyber crime i.e. Identity Flexibility, Dissociative Anonymity and lack of Deterrence etc.
- The behavior of offenders which is criminal in nature
- Intermittent ventures of offenders
- Closed society’s persons are more interested to commit crimes in cyberspace rather than persons from open society.
- The conflict between Norms and Values of Physical Space with cyberspace

---

3.6.4 Structural-Functional Theories

The key insight of the structural-functional theory is that crime and deviance is a necessary part of social organization. It maintained that society is an organism, a system of parts, all of which serve a function together for the overall effectiveness and efficiency of society. Structural-functionalism is a consensus theory which sees society as built upon order, interrelation, and balance among parts as a means of maintaining the smooth functioning of the whole.\textsuperscript{64} The theory mainly focuses on social order which is based on tacit agreements between groups and organizations and also focuses on the views base on social change as occurring in a slow and orderly fashion. This theory also provides us insight understanding that crimes and deviance is not a matter of a few bad peoples but it is necessary condition of good social living.

In this theory, Merton tries to highlight a strain between:

1. The cultural goals of a society
2. The legitimate or institutionalized means to achieve these goals

3.6.5 Routine Activity Theory

The Routine Activity Theory was proposed by Cohen and Felson in 1979. They contended that for a crime to take place three requirements needed to be present; a motivated offender, a suitable target, and absence of capable guardians. The theory argues that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. Crime does not needs hardened offenders, super-predators, convicted felons or wicked people.\textsuperscript{65} According to him, crime only wants an opportunity to commit. This theory provides us the knowledge about the reason of engaging in cybercrime. By the systematic study we can get an idea that why peoples are involving day-by-day in the commission of cyber crime.

Pratt, Holtfreter, and Reising points out that while Routine Activity Theory suggests that victims engaging indeviant behaviour are more likely to be victimized victims of online auction fraud are typically involved in legitimate, lawful behaviour at the time.

\textsuperscript{64} Supra note 62, p. 119.
\textsuperscript{65} Ibid.
of victimization. Because of this, simply engaging in procuring items from online auction sites is a high-risk behavior compared to individuals that do not buy items via online auctions. In essences, although it is not unlawful, the behavior of buying items through online auctions is not the norm. Further, since the routine activities perspective was proposed after the introduction of the lifestyle exposure theory and it encompasses not only the theoretical element inherent in the lifestyle exposure theory but also two additional elements, routine activities theory is thus perceived as an extension and more general expression of the lifestyle exposure theory.

3.6.6 Theory of Technology-Enabled Crime

McQuade reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there is continual competition between the criminals and law enforcement for technological advantage. As criminals do something new and innovative, law enforcement must catch up in order to avert, control, deter, and prevent new forms of crime. The theory provides a framework for understanding all forms of criminality and especially those that are evolving with computing and telecommunications technology inventions and innovations. This theory help the society by combining several categories of criminological theories for the better understanding that the computer and telecommunications technologies are becoming more complex and difficult and also the preventive methods for investigation and controlling these forms of crime on cyber space. The theory also provides for better understanding of threats posed by emerging forms of cybercrime and also suggests the methods for criminal justice and security measures for preventing such crimes.

According to McQuade, technology-enable crime theory encompasses that:

1. Commission of crime directly against computers and computer systems.
2. Use of this technology to commit or to facilitate the commission of traditional crimes
3. Bringing the unique challenges to old crimes.

---

66 Supra note 61, p. 915.
68 Supra note 64.
3.7. Meaning and Concept of Cyber Crime

The term ‘Cyber’ the use of which became universal by the 1980s finds its origin several decades earlier when Norbert Wiener coined the term ‘cybernetics’ in 1948 and described the same as ‘the study of message as a means of controlling machinery and society’⁶⁹ In fact the term ‘Cyber Crime’ is frequently used in 21st century knowledge society and is created by combination of two words cyber and crime. The term Cyber denotes the cyber space i.e. virtual space and it means the informational space modelled through computer, in which various objects or symbol images of information exist. Therefore, it is the place where the computer programs work and data is processed.⁷⁰

Cyber crimes are nothing but crimes of the real world perpetuated in the medium of computer and hence there is no difference in defining a crime in cyber world and real world. Only the medium of crime is different.⁷¹ Cybercrime is "international" or "transnational" – there are ‘no cyber-borders between countries’.⁷² Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is source, tool, target or place of crime as well as traditional crime through the use of computers like child pornography, Internet Fraud. 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.⁷³

Cyber crime is multiplying like mushrooms.⁷⁴ Broadly speaking, it is also stated, ‘cybercrime’ can be said to be an act of commission or omission, committed on or through or with the help of or connected with, the internet, whether directly or indirectly, which is prohibited by any law and for which punishment, monetary and/or corporal, is provided.⁷⁵

---

⁷⁰ Supra note 7, p.215.
⁷³ Supra note 71, p.85.
⁷⁵ Supra note 18, p.43.
To put it in simple terms, cyber crime means any offence or crime in which a computer is used. Some expert says that cyber crimes are nothing more than ordinary crime committed by high tech computers. Other says that cyber crimes are as a new category of crime requiring a comprehensive new legal framework to address the unique nature of emerging technologies and unique set of challenges that traditional crimes do not deal with. States have believed cybercrimes as both traditional crime committed by new methods and as crime is unique in character requiring new legal framework.

Cybercrime has a narrow statutory meaning as used in the Cybercrime Act, 2001 of Australia, which details offences against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's Cybercrime Treaty cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. The U.S Department of Justice, in its manual on computer crime, defines such crimes as any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.

3.8. Definition of Cyber crimes

The term 'Cyber Crime' is a misnomer. It is used as a generic term which refers to all criminal activities done by using the computers, the Internet on cyber space and the worldwide web. In India, any definition to the term ‘cyber crime’ has not given yet in any law. In fact, the Indian Penal Code, 1860 does not use the term ‘cyber crime’ at any point even after its amendment by the Information Technology (Amendment) Act, 2008.

"In the absence of a common definition of the notion of 'cybercrime' in the legal framework of the European Union, several measures planned in the Strategy relating

---

76 EST no. 185
to the fight against 'cybercrime' (such as measures to strengthen cooperation amongst law enforcement bodies) are not clearly linked to precise and well-defined offences.”

Cyber crime may be defined as “Any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime.” An online dictionary defines “cybercrime” as “a crime committed on a computer network.” Cybercrimes can be plainly defined as “crimes directed at a computer or a computer system.” But the complex nature of cybercrimes cannot be sufficiently expressed in such simple and limited terms. According to Pavan Duggal, Cybercrime refers to all activities done with criminal intent in cyberspace or using the medium of internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activities which basically offend human sensibilities can be included in the ambit of cybercrimes.

The United Nations Manual on the prevention and control of computer related crime defines the cybercrime as “computer crime can involve activities that are traditional in nature, such as theft, fraud, forgery, and mischief, all of which are generally subject everywhere to criminal sanctions.” The computer has also created a host of potentially new misuses or abuses that may, or should be criminal as well. Thus, a better definition of cybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society’s ability to maintain internal order. This definition encompasses both traditional and emerging cybercrimes. It also encompasses any use of computer technology, not merely the use of networked computer technology.

---

84 Supra note 19, p.89.
85 Pawan Duggal, Cyberlaw- The Indian Perspective, 2002, p. 256.
87 Supra note 82, p. 386.
3.9. Nature of Cyber Crimes

Cyber crime is multiplying like mushrooms.\textsuperscript{88} Cyber crimes include crimes which are specific to computers such as hacking; e-mail spamming and denial of service attacks, as well as conventional crimes committed using a computer, such as theft, fraud and extortion. As a result, a cyber crime may invite the application of not only legislation, which is the Information Technology Act, 2000, but also general criminal legislation, which is the Indian Penal Code, 1860. Other laws will also be applicable depending on the nature of the crime.\textsuperscript{89}

Prof. S.T. Viswanathan has explained the nature of cyber crimes as follows: firstly, any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer. Secondly, any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain. Thirdly, computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data.\textsuperscript{90} According to Loader B.D., a flexible communications system designed to withstand attack by means of rerouting message has also proved difficult for governments to control. Sources of illegal activity often require advanced computer skills to be detected as a consequence of their anonymous character.\textsuperscript{91}

Cybercrimes are made possible by the combination of computers with telecommunications abilities. The power to send data over communications equipment has transformed our society completely. This capacity to send data, however, does not operate in a perfect world. An analogy might be that ever since the first lock was invented, there have been criminals trying to pick the locks. And so it is in the information age. Even as data is being sent, criminals may be trying to steal or manipulate it; use it as ransom; spy on, or copy it. Even as early as 1998, the FBI considered that cybercrime was becoming epidemic. These computer criminals, which

\textsuperscript{88} Supra note 74.
\textsuperscript{89} Supra note 8, p. 82.
\textsuperscript{91} D. Thomas and B.D. Loader, Cyber Crime Law Enforcement, Security and Surveillance in the Information Age, 2000, p. 3.
are anonymous in a virtual world, will be the next significant wave of crime perpetrators.\textsuperscript{92} A computer is a subject matter, it can be victim, it can be the facilitator and it can be the instrument of a crime.\textsuperscript{93}

The nature of cybercrime and the legal issues are global. Through international organizations, such as the G-8 Group, OAS (Organization of American States), APEC (Asia-Pacific Economic Cooperation) and the Council of Europe, efforts have been taken to ensure the harmonization of provision in the individual countries. Ensuring that the dual criminality requirement is fulfilled may provide for an efficient global prosecution of cybercrimes. Such an approach is especially vital in the investigation and prosecution of attacks against the infrastructure of computer systems and networks.\textsuperscript{94} By nature cyber crimes are different from other types of crimes which are discussed as follows:

The words “Cybercrimes” and “Computer crimes” are used interchangeably in common parlance. The word “Computer crimes” has wider ambit as it entails not only crimes committed on the Internet but also offences committed in relation to or with the help of computers.\textsuperscript{95} Most people are confused about the difference between cyber crime and computer crime. Even cyber crime authors do not always appropriately separate the terms.\textsuperscript{96} Therefore, it is necessary to define the difference between cyber crime and computer crime. Computer crimes generally include crimes whose perpetrators utilize a computer or computers to commit them, and cybercrimes are those crimes that involve a computer network.\textsuperscript{97}

Donn B. Parker distinguishes between the concepts of computer crime and cyber crime. Computer crime is a crime in which the perpetrator uses special knowledge

\textsuperscript{92} \textit{Supra} note 18, p. 47.
\textsuperscript{93} \textit{Supra} note 1, p. 9-10.
about computer technology but in cyber crimes, the perpetrator uses special knowledge of cyberspace. In general, special computer operating skills are not required to commit cyber crime. For example, in cyber crime, a suspect and a victim may communicate via Web based chat-rooms, Microsoft Network Messenger (MSN), or e-mail. Once the criminal gains the potential victim’s trust, the criminal is in the position to commit a crime against the victim. In this case, even though the Internet probably assisted the suspect in communicating with the victim, it does not mean that the technology or the Internet caused the crime.

3.9.1 Distinction between Cyber Crime and Traditional Crime

Cybercrimes, uniquely different from traditional crimes, are often harder to detect and prosecute. The Swedish Emergency Management Agency’s 2008 report, “Information Security in Sweden: Situational Assessment,” observes that criminal activity on the Internet has become progressively more sophisticated. Perpetrators carry out cybercrimes through small, targeted Internet attacks, as well as launching significant attacks using large networks of commercially leased, hijacked computers. Chen Junjiing, researching the legal issues of cybercrime in China, concludes that these crimes are more widespread than traditional crimes and are increasing at a faster rate. Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate.

Cyber crime encompasses any criminal act dealing with computer and networks. Additionally, cyber crime 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. The hackers in cyber crime are professional thieves, criminal gangs, disgruntled employees, professional competition, activists, disillusioned youth and state adversaries as compared to traditional crimes.

---

101 Ibid.
The other difference between these two terms is based on the evidence of the
offences. In the traditional crimes the criminals after or during the commission of
crime usually leave any proof of that crime like fingerprints or other physical proof.
But in the cyber crimes the cybercriminals commit their crime through internet and
there are very less chances of leaving any physical proof. According to the Forensic
investigators usually having the experience of difficulty in gathering evidence for the
conviction of cybercriminals because after the commission of crime they change their
identities or doing the crime on the basis of fake identities of others. But as compare
to traditional criminals it is very difficult to fake their gender, race, or age etc.

These two terms can be differentiated on the basis of use of force. In the traditional
crimes many of the crimes like rape, murder, and burglary etc. involve the use of
excessive force which leads to physical injury on the suffered person. But as compare
to cybercrimes there is no requirement of using any type of force because in this type
of crimes the criminals only use the identities of other person for the purpose of
stealing any secret information etc.

3.10. Characteristics of Cyber Crimes

Characteristics are the main concern by which we can differentiate a thing from other.
Like other crimes, cyber crimes have also some different characteristic which makes
it separate from the other types of crime. The main characteristic of these crimes are
explained as under:

Cyber crimes are silent in nature. This crime could be committed in the privacy of
one’s home without the need to physically reach the victim and with no eye witnesses.
There are no signs of physical violence or struggle at the scene of crime, no cry of
pain etc., which are the usual hallmarks of traditional crimes.\(^3\) This is the first
characteristic of the cyber crime in which a cyber criminal silently commits the crime
without any sound or without any afraid of being caught red handed. These crimes
can be committed with a single click on the mouse and without the knowledge of the
victim of such crime. In most of cases of this type of crimes the victim will not even
realise what has happened to him and who have done it against him and when it was

\(^3\) \textit{Supra} note 18, p. 48.
done. This is rightly said that the nature of the blow of this crime would be swift, silent and with a killer punch.

Cyber crimes are Global in character. In the era of liberalization and globalization we must recognize cyber crime as significantly new phenomena which have political, social and economic impact worldwide. The global connectivity of internet makes possible for existing organized criminals to use sophisticated techniques to communicate between groups and within a group to support and develop networks for illegal arms trafficking, money laundering, drugs trafficking, pornography and other cyber crimes. 104 Due to this nature of cyber crimes, any cyber criminal commits a crime from any place globally. There is no need to go the victim place for committing crime against him.

This type of crime creates high impact. In the case of bank robberies, for example, the quantum of losses is constrained by the weight, and volume of currency that can be carried away by the burglars. The amount burgled does not close down the bank operations permanently. The chances of robbery taking place again in the same bank are remote since it is possible to take suitable precautionary measures and revamp the security of the bank. The loss of goodwill is also not very huge. On the contrary, in case of computer crimes, its impact is severe and it is not a one-time blow but may be a long-term one. It could cripple the operations of the victim and in most of the cases maim them permanently. More than the financial loss, it is the loss of faith of the customers that would deliver the knockout punch, especially in case of companies whose main businesses are dependent on the internet, i.e., on e-commerce. The customers could lose faith on the seller and all the investments made to gain that trust is lost through the action of a few clicks. 105 These crimes are also high potential and easy to perpetrate.

Low risk and high rewarding ventures are another characteristic of cyber crimes. The most striking feature of cybercrime is that they are relatively easy to commit, difficult to detect and even harder to prove. The cyber criminals with basic computer knowledge and skill can easily destroy valuable database causing huge loss or damage

104 Supra note 1, p. 8.
105 Supra note 103.
to the affected victims of the crime.\textsuperscript{106} That’s why this feature makes this crime different from other types of crimes. This feature of low risk having high rewarding ventures can be seen in a very less types of crimes.

Many a times it happened that the party or the organization victimized by the cybercrime prefers to refrain from reporting it to the police for the fear of adverse publicity or possibility of the loss of public trust in them. The unwillingness and hesitation of the victims to come forward and file a police complaint against the cybercriminal further aggravates the magnitude of the problem of cybercrime detection and control.

The other characteristic of the cyber crime is the non-existence of physical evidence in the commission of cybercrime. In case of computer crime, the crime scene does not yield any such physical evidence to indicate that the crime has been committed. The place remains clean and tidy and there are no signs of disturbance.\textsuperscript{107} This is the plus point in favour of the cyber criminals that by committing such crimes there is no existence of any physical evidence against him and as the negative point against the victim because he has to face many hurdles for proving the crime against him without any physical evidence.

3.11. Category of Cyber Criminals

“Amidst the surging excitement and interest, however runs a deep thread of ambivalence towards connecting to the internet. The internet’s evil twin is the home of “Bad Guys”-hackers, crackers, snackers, stalkers, phone preaks and other creepy web crawlers. Business fear that the Infobahn could suddenly veer into the highway to Hell.”\textsuperscript{108}

The emerging information and communication technology inevitably has an immense impact on the life of the people in modern time, but the advantages and benefits global connectivity has brought with them certain dangers emanating from inter-connectivity of information networks which provide scope for cyber criminals to

\textsuperscript{106} S.K. Bansal, Cyber Crime, 2003, p. 17.

\textsuperscript{107} Supra note 103.

carry on their criminal activities in cyberspace. A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. For example, hackers were once more often than not hobbyists who broke into systems for personal gratification. While white-hat hacking hasn't disappeared, it's much more common now to see hackers as professionals who sell their services to the highest bidder.

Cybercriminals tries to use the computers in three broad ways, firstly, they use the computer as their target for attacking other people's computers for the purpose of fulfilling their malicious activities like spreading viruses, data theft, identity theft, etc., secondly, they uses the computer as their weapon for the purpose of carrying out conventional crime like spam, fraud, illegal gambling, etc., thirdly, they uses the computer as their accessory for the purpose of saving stolen or illegal data.

Unlike traditional offenders, the cyber criminals are hi-tech knowledgeable persons who invade rights of computer users by unauthorized access to their computer system or computer network. Usually, they indulge in techno-vandalism by unauthorized access which causing damage to files and programs of the computer user. They are engaging in this type of activities not necessarily for monetary gain but also may be prompted by an adventure or may be for the purpose of harassing the victim.

The age-wise profile of persons arrested in cyber crime cases under IT Act, 2000 showed that 62.5% during 2015 and 52.7% during 2014 of the offenders were in the age group 18 years, 3,188 out of 5,102 persons during 2015 and 2,238 out of 4,246 persons during 2014 were below 30 years and 30.08 % during 2015 and 39.1 % during 2014 of the offenders were in the age group 30 years, 1,573 out of 5,102 during 2015 and 1,660 out of 4,246 during 2014 persons were below 45 years and 98 during 2015 and 67 during 2014 juvenile offenders were apprehended under IT Act. A total of 3,502 persons during 2015 and 1,931 persons during 2014 charge sheeted. A total of 250 person during 2015 and 65 persons during 2014 were convicted and

---

111 Supra note 45, p. 42.
358 persons during 2015 and 165 persons during 2014 were acquitted under cyber crime cases.\textsuperscript{112}

The following are the category of cyber criminals on the basis of the object because the cyber criminals constitute of various groups or category:

3.11.1 \textbf{Children and adolescents between the age group of 6 – 18 years}

Cyber criminals are teenagers who do not know that what they are doing is an act prohibited by law or is a crime. The reason for this kind of delinquent behaviour among children and adolescents are mainly due to inquisitiveness and curiosity of knowing and craze for grasping new things. For them, it is an adventure or fun to hack into someone’s computer system or website. Other cognate reason may be to prove themselves over-smart among their friends and colleagues. Adolescents may also be psychologically motivated to explore new website by unauthorized access without really knowing that they are doing a criminal activity.\textsuperscript{113} The main reason for this delinquent behaviour which is seen in children these days is mostly due to the willingness to know and explore the new things through internet. The other reason may be to prove them to be outstanding amongst other children in their group.

3.11.2 \textbf{Organised Hackers in Cyberspace}

Organised criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organisations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged.\textsuperscript{114} For the purpose of e-business a huge amount of data are secured and stored in the computers and the industrial management for storing data in electronic form has led these enterprises to employ some hackers to steal the credible, reliable and valuable information for the purpose of commercial gain. In this category, the organised hackers are also employed to crack the system of the employer as a method for providing it safer by detecting all the ambiguities.

\textsuperscript{112} National Crime Records Bureau, Ministry of Home Affairs, cyber Crimes in India, 2015, available at: http://ncrb.nic.in (visited on Nov. 11, 2016)
\textsuperscript{113} Supra note 45, p. 43.
Hackers are mostly organized together to accomplish certain objective. Hacktivist are the hackers with a particular motive which may be to avenge their political bias, fundamentalism or an act done for some big business organization for causing damage to its rival competitors. Their work is motivated by the colour of money. In this category of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information.

A recent paper sponsored by the RAND Corporation’s National Security Research Division, titled “Markets for Cybercrime Tools and Stolen Data”, said the increasing size and complexity of cybercrime black markets is because the hacker market, “once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety, has as a playground of financially driven, highly organized and sophisticated groups”. 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. These types of cyber criminals mainly focused on money but there is always a little mystery about where is the money by using to cyber.

3.11.3 Discontented Employees

This category of employees includes those persons who have either been sacked by their employers or are reprimanded for their nefarious activities. In order to avenge their discontentment, these persons generally resort to hacking the computer system of their employers to cause him financial loss or damage. With the extensive use of computers and automation processes in modern times, it is easier for the disgruntled employees to do more harm to their employers by hacking the computer which can bring the entire system down and thus paralyze the employer’s business related activities. This is due to the lack of trust by the employers on the employees, poor

117 Supra note 45, p. 44.
communication between them and unlawful behaviour to each other is the main factors responsible for the employees discontented. It will lead for increasing negative relationship between them and encouraging for involvement in crimes.

3.11.4 The Typical Cybercriminal

In this category of cyber criminals includes those persons who use computers and networks for the purpose of committing crimes. Almost in every case there are exceptions to the characteristics of this category of persons but most of cybercriminals have some characteristics firstly including that some of them having the measure of technical knowledge i.e. using others' malicious code, secondly, some of them are disregarded for the law or rationalizations and having the question in their mind about why particular laws are invalid or should not apply to them, thirdly, some of them have the characteristic of high tolerance for risk, fourthly, having the control freak nature, and lastly, some of the cyber criminals have the motive to commit the crime for monetary gain, strong emotions, sexual impulses, political or religious beliefs, or having the desire for fun and enjoyment.

3.12. Classification of Cyber Crimes

The computer related crime has already become an area of serious concern for most of the countries of the world, and India is no exception to it. The prime factor that has to be taken into consideration while deciding whether a particular computer related activity be reckoned as cyber crime is that a distinction must be drawn between what is unethical and what is illegal. Gabriel Weimann, an Internet and security expert who teaches in the University of Mainz in Germany and has studied militant’s use of website for nearly a decade, while addressing the Internet security personnel said that, “website and chat room used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda but also for terrorist education. Al-Qaida has launched a practical website that shows how to use weapon, how to carry out kidnapping and how to use fertilizers to make a bomb. 

The incidence of cyber crime is directly proportional to the level of progress made by a country in computer technology. The report of the United Nations stated that more than 50% of the websites in the United States, Canada and European countries have

experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies. A new trend that has developed in recent years is that the militants are going for terror training. The Internet has become a key teaching tool for militants who are using it to educate recruits in cyber terrorist’s training camps.\textsuperscript{120} Due to the global in nature these types of crime are expanding globally day-by-day and affected the huge amount of peoples at the same time.

In the absence of an internationally recognized definition of cybercrime or computer crime, there has been a great deal of debate amongst the legal experts on the term ‘computer misuse’ practice in vogue in this regard is to hold that the 2 terms have different implications. The criminal law applicable to cybercrime must make a distinction between incidental misuse of a computer system, negligent misuse and intentional misuse of computer system and it is the later, which should be treated as a crime and not the former two.\textsuperscript{121} This is the misuse of a computer system which should come under the criminal activities and should be punishable under law.

In this technological world, most of the people have no knowledge regarding which types of crimes come under the cyber crime. There are two sides to cyber crime. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that, the number of cyber crimes committed should be related to the number of victimizations experienced of course there will not be a one-tone correspondence since one crime may, inflict multiple victimizations multiple crimes may be responsible for a single victimization. Some crimes may not result in any victimization, or at least in any measurable or identifiable victimization.\textsuperscript{122} The usual effect of this type of crime is the evolving threat on business and the motive of these attacks has been changed over time in place of gaining fame.

There are a number of controversial issues surrounding cybercrime. Opinions differ, for example, as to whether some widespread activities should be classified as criminal


\textsuperscript{121} Supra note 45, p. 57.

acts. The all types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target.\textsuperscript{123} Cyber crimes can be broadly classified under various categories which are as follows:

\textbf{3.12.1 Cybercrimes against Individual}

The term crimes against the individual refers to those criminal offences which are committed against the will of an individual like bodily harm, threat of bodily harm generally including assault, battery, and domestic violence, harassment, kidnapping, and stalking etc. but in reference to cybercrime this category can be in the form of cyberstalking, distributing pornography, trafficking, cyber bulling, child soliciting and abuse. Such cybercrime affects the individual’s personality and affect the psychology of younger generation in a unlawful manner. These are as following:

i. Unauthorized control/access over computer system

ii. Dissemination of obscene material

iii. Cyber-stalking

iv. Indecent exposure

v. E-mail Harassment

vi. Defamation

vii. Cheating & Fraud

viii. Email spoofing

\textbf{3.12.2 Cybercrimes against individual's Property}

The second category of cyber crime is that of cyber crimes against all types of property. As there is rapid growth in the international trade where businesses and consumers are increasingly using computer to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects person’s property. These cybercrimes are known as cybercrimes against property.

These types of cyber crimes include cyber vandalism to steal database of other organizations with the help of corporate cyber spy for spreading harm. Like in the real world, a cyber criminal can also steal a person’s bank details; misuse the credit card for online purchasing; use software to gain access to an organization’s website for disrupting the systems of the organization etc.

### 3.12.3 Cybercrimes against Government or Organization

There are certain offences done by group of persons intending to threaten the international governments or firm, Company, Group of Individuals by using internet facilities. These cybercrimes are known as cybercrimes against Organization. As compared to other two categories, cyber terrorism is referred as crimes against a government. Cybercrimes against Government includes cyber attack on the government website, military website or cyber terrorism etc.

These crimes are committed for the purpose of spreading terror among people of a particular country by circulating false information. This category can cause panic amongst the civilian population if successful. In this category of cyber crime, cyber criminals hack Company websites, government firm, and military websites or circulate propaganda. The perpetrators can be unfriendly governments of other nations or a terrorist outfits. This includes:

i. Cyber terrorism  
ii. Possession of unauthorized information  
iii. Unauthorized control over computer system  
iv. Distribution of pirated software  
v. Cyber vandalism.  
vi. Virus  
vii Net-trespass  
v. Intellectual Property related crimes  
vi. Cyber thefts

### 3.12.4 Cybercrimes against Society

Those cybercrimes which affects the society interest at large are known as cyber crimes against society. These unlawful acts are done with the intention of causing to
the cyberspace which will automatically affect the large number of peoples. The main target of these types of crimes is public and to create the fear in the mind of the public which would result in the causing fear to government. The cyber crimes against society include the following types of crimes:

i. Cyber Pornography

ii. Online gambling

iii. Financial cyber crimes

iv. Cyber Trafficking

v. Cyber Forgery

3.12.5 Computers as a Tool in the Commission of Cybercrimes

In this category of cybercrime, a computer is used as a tool to commit the cyber crime. When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. For committing this type of cybercrimes, the role of computer is same as played by the telephone in telephone fraud.

In this category of cyber crime, computer is used as the means of committing cyber crimes. For committing cyber frauds, hackers modify the computer programs. In this category of cyber crime includes the credit card frauds, online fund transfers and stock transfers, Scams, theft etc. The following are the cybercrimes included in this category:

i. Credit Cards Fraud

ii. Electronic funds transfer fraud

iii. Fraudulent use of Automated Teller Machine (ATM) cards and accounts

iv. E-Commerce fraud

v. Telecommunications fraud

vi. Stock transfers fraud etc.

3.12.6 Computers as a target in the Commission of Cybercrimes

When a computer is the target of crime, the perpetrator attacks the computer by breaking into it or attacking it from outside. This is the most professional as comparing in three cybercrime, because the criminal does programming and makes use of some exploits on computer, who always has pretty strong professional background of computer science.
This type of cyber crimes are committed only by a selected group of cyber criminals. These crimes require the technical knowledge of the cyber criminals as compared to crimes using the computer as a tool. The main purpose of committing these cyber crimes is to directly cause damage to a computer system or to access the important data stored in a computer. This includes stealing data or information from system, theft of computer software, blackmailing based on persons information gained from computer etc.

i) Intellectual Property Theft;

ii) Marketable information theft;

iii) Theft of data/information;

iv) Sabotage of computer, computer system or computer networks;

v) Unlawful access to government records and criminal justice etc.

3.12.7 Computers as incidental to Cybercrimes

In this category of cyber crime, a computer has a minor role in committing the cyber crime. This includes hacking, cyber stalking, spamming, gambling, insurance frauds, pornography, threats by e-mails etc.

i) Internet Crime are those crimes which includes the group crimes that make the criminal use of the internet infrastructure like hacking, spamming, Espionage etc.

ii) Web based Crime are those crimes which includes crimes relating to website, e-mail, internet chat i.e. cheating, pornography, insurance fraud, extortion, e-mail bombing, gambling, forgery, spoofing, cyber squatting, sale of pirated software, defamation, sale of stolen data, cyber stalking, illegal access etc.

3.12.8 Cyber Crime under Information Technology Act, 2000

Indian Parliament has passed the first legislation which is specifically deals with cybercrimes. The legislative provisions relating to cyber crimes are given under Chapter XI of the Information Technology Act, 2000 titled as ‘Offences’ which deals with the various types of offences which is done in the electronic form or concerning with computers, computer systems, computer networks. Strangely, the term ‘cyber crime, or ‘cyber offence’ is neither defined nor this expression is used under the
Information Technology Act, 2000. Hereunder are mentioned those cyber crimes which are punishable under the Information Technology Act, 2000. These are as follows:

i. Tampering with computer source documents  
ii. Computer related offences  
iii. Sending offensive messages through communication service  
iv. Dishonestly receiving stolen computer resource or communication device  
v. Identity Theft  
vi. Cheating by personation by using computer resource  
vii. Violation of privacy  
viii. Cyber terrorism against the government organization  
ix. Publishing of information, which is obscene in electronic form  
x. Failure to comply with the directions given by Controller  
xii. Access protected system  
iiii. Breach of confidentiality and privacy  
xiii. Disclosure of information in breach of lawful contract  
xiv. Offences related to Electronic Signature Certificate  
xxv. Offences by Companies  

13. Factors Responsible for Cyber Crimes

Professor H.L.A. Hart in his classic work entitled ‘The Concept of Law’ has stated that human beings are vulnerable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Applying the same analogy to cyberspace, the computer systems despite being hi-tech devices, are extremely vulnerable. This technology can easily be used to dupe or exploit a person or his computer by illegal or unauthorized access. The damage so caused to the victim may be direct or indirect result of abuse of computer systems. In the absence of any foolproof mechanism to protect and safeguard innocent computer users against cyber criminality, the cyber criminals indulge in criminal activities through networks unabated without any fear of being apprehended and tried for the offence committed.
The following are the factors responsible for the emergence of cybercrimes.

Huge Data Storage Capacity is the first reason which is responsible for the emergence of cybercrimes. The computer has a capacity to store huge amount of data on a small space. A small micro-processor computer chip can store lakh of pages in a CD-ROM. The data stored in ROM will always remain safe and not destroyed even if the power is turned off. A cyber criminal can intentionally get the large scale of secret or official data from the other person personal computer within a few minutes. This leads to increasing cyber crimes.

Computer System’s Complexity is the second factor which is responsible for the emergence of cybercrimes because the computers work through operating systems which are composed of millions of codes. Due to the fallible nature of Human’s mind there is always a chance for lapse at any stage of processing. The cyber criminal’s are always ready to take undue advantage of these chances of lapse and get access into the computer system. These types of criminals are known as hackers on the cyber space who tries to exploit the weaknesses in existing operating systems and security devices.

Negligence of Network user is the third reason which is responsible for the emergence of cybercrimes because negligence is closely related to human conduct. There is always a probability that there might be any negligence on the part of network user while he is trying to protect the computer system. This negligence leads to a chance for the cyber criminal to gain unauthorized or illegal access or control over the computers and commits crime. Evidence unavailability or loss is the fourth reason which is responsible for the emergence of cybercrimes. Now the digital computer processing and network technology has replaced the traditional methods for producing, storing, transmitting and disseminating information or records. Due to the emerging nature of cyber crimes the issue raises before the law enforcement and investigating agencies is for procuring and preserving evidence against the cyber criminals. As compare to traditional offences, it is very difficult to collect sufficient evidence of a cyber crime for found him guilty of the cyber crime beyond doubt. Due

---

to the anonymity, providing by internet, the cyber criminals are encouraged to indulge in criminal activity without leaving any evidence and if in some cases the evidence is left then it is hardly possible to convince the police for registering a case against that criminal.

In the modern time period due to the inadequacy of traditional methods of evidence and crime investigation it becomes necessary to adopt the new techno-legal procedure called cyber forensics. In the cyber crimes, the forensic experts are playing an important role in collecting and presenting admissible electronic evidence and search and seizure of material evidence relevant to the cyber crime under investigation. Instead of this hard work there are still certain grey areas which enable the cyber criminal to make tampering with the evidence for the purpose of misleading the investigating agencies.

Wider access to information is the fifth reason which is responsible for the emergence of cybercrimes. Computer is defined as an electronic device which performs function through complex technology rather than manual actions of human beings. The wider access to information resources is the greatest advantage of computer networking in the cyber age. More and more organizations are resorting to networks for providing easily accessible information to their employers, customers and parties with which they deal. In the present information age this is the reason why networking and cyber activities are increasing day by day. Due to the information dissemination through World Wide Web, new resources have been created for faster and cost effective access to information throughout the world. This facility leads to involve in crime commission on the cyber space.

Jurisdictional uncertainty is the last factor which is responsible for the emergence of cybercrimes. Cybercrimes cut across territorial borders which undermine the feasibility and legitimacy of applying domestic laws which are normally based on geographic or territorial jurisdiction. Cybercrimes are committed through cyberspace network interconnectivity and therefore, they do not recognize geographical limitations because of their transnational in nature. There has been no uniformity in

law of procedure among the different countries for dealing with cyber criminals. Sometimes the issue rose that a particular cyber activity is recognized as a crime in one country where it is committed but it is not so in the country in which the criminal or the victim resides due to this lack the criminal easily escapes from the charge under cyber law. The law enforcing authorities find it very difficult to deal with cybercrimes in the absence of a single internationally recognized code of law and procedure governing cyber crimes.

In criminology, it has been rightly said that a crime will happen where and only when the opportunity avails itself. Before this we were known only about the traditional types of crimes like murder, rape, theft, extortion, robbery, dacoity etc. But now with the development and advancement of science and technology i.e. computers and internet facilities, new types of crimes exist like hacking, cyber pornography etc. The science, new technology and internet have opened a new virtual heaven for the people both good and bad to enter and interact with lot of diverse cultures and sub-cultures. But in future, it will make a virtual hell for everyone when the internet gone in wrong hands or when used or controlled by the peoples having dirty minds and malicious intentions. Due to such utility of information technology and internet, the cyber criminals and terrorists used the computer as a target or a tool for committing such types of crimes.