CHAPTER - 2

REVIEW OF LITERATURE
AND THEORETICAL
FRAMEWORK OF THE STUDY.
CHAPTER-2

REVIEW OF LITERATURE AND THEORETICAL FRAMEWORK OF THE STUDY

2.1 REVIEW OF LITERATURE

The present research is designed to study the extent of cyber crimes and the Importance of the Information Technology Act-2000, with a criminological perspective. The area of the research has been Bangalore City. The research further takes into the various aspects of cyber crime in relation to the Information Technology Act- 2000 into consideration. An efficient law enforcement system is as good as the structure of the law. Thus, the study also undertakes pertinent issues related to the Cyber Crime Police Station, Bangalore.

Computers are an integral part in the world. No society or country can simply exist without this aspect, in today’s fast developing and globalised world. Computers, computer networks and systems have become a vital part in Banking, Trade, Commerce, Insurance, Defence, Health care management and even governance. This apart, it is seen in Scientific Research, education and generally, office automation. E-Commerce has been enabled by the vast growth of computer networks, which has rendered the world, flat, bringing about outsourcing of business processes to several countries of the world.
In this era of technologically driven enterprises, Banking and commerce transact trillions of dollars every day and millions of messages traverse the globe, via the Wide area Network every hour. In addition to this, computers, Computer Systems and Computer Networks are extremely vital for all Governments, Military, Industries and above all Trade and Commerce.

Speed of dissemination of information, comfort and accuracy in its handling large quantities of data, several operations can be executed simultaneously, virtually rendering paper documents to redundancy and capacity to store and retrieve large quantities of data and above all, doing it accurately has rendered computers as a vital element in all our every day lives.

Like in any free and unhindered trade, there are regulations for ethical practices and to avoid malpractices, Laws are legislated. The Cyber space also has its laws to recognise and regulate trade related activities in the computer networks, by using computer systems. It also is to cover the darker aspect of the computer revolution; as many of the computer applications are likely targets for crimes. These crimes vary from traditional crimes such as theft, extortion, fraud, vandalism to newer types of technologically driven crimes such as hacking, illegal intrusion into
computer system and Malware. They are also susceptible to many different forms of criminal activities or to facilitate crimes such as money laundering, drug trade, human trafficking and other forms, that have fallen in the class called Organised Crimes. There are several types of White collar crimes that are included within the scope of Cyber Crimes or Computer Crimes.

Till the past decade, the attitude of the various types of users was casual and relaxed with regard to the protection of computers, computer systems and computer networks. It was always felt that the threat was exaggerated.

Losses due to cyber crimes globally has prompted the corporate sector, defence and other governmental agencies to enhance their efforts in dealing with this complex phenomena of offences, which are conjointly called as Cyber Crimes or Computer Crimes, interchangeably in the literature which the researcher has referred to.

Few of the literature which the researcher has reviewed are as following:

Aj. Singh, Pramod Kumar (2007)\textsuperscript{15} traces the origin of the term “Cyber Space” as coined by William Gibson in the science fiction novel “Neuromancer” in 1984. Basically, it denotes the virtual location within

\textsuperscript{15} Singh, Pramod Kumar; “Law on Cyber Crimes” (P.4-11, 14-16 & 40-63) Book Enclaves; New Delhi. (2007)
which the electronic activities takes place. Cyber space is a borderless environment. It has no territorial based boundaries. The internet address has no relation to the physical location of the computers and individuals accessing to them thus render geographic borders of nations meaningless. Cyber space, thus, challenges the well established principles of international law that controls over the physical space and people is an attribute of sovereign and statehood.

B. Bequal (1979) brings out the necessity of Cyber Laws or laws relating to the use of information technology that the problem has been aggravated by the antiquated and over-bureaucratized legal apparatus. At stake is the very form of government, and if there is a failure to adapt the legal systems to the needs and demands of an ever growing technology, the entire system of governance would collapse.\(^{16}\)

C. According to Bologna (1981), the literature of computer crime is loaded with theft, motivation and rationales. He provides professionals in the field of computer crime detection, audit, investigation and prosecution a systematic look into the causation of theft. He has proposed a classification

\(^{16}\) Bequal, August, "computer Crime" Lexington books: Toronto; 1978.
for causation of computer thefts related to employees: (1) Motivation. (2) Opportunities. (3) Means. (4) Methods.¹⁷

Dl. Ghokale and Pawar (1994)¹⁸ have suggested that it is imperative for a developing country like India to focus their attention on this phenomenon, and introduce necessary amendments to the existing laws, and if need be, enact new laws, so that computer crime can be tackled in time. This also facilitates the expanding horizons of traditional criminology. The argument is that law in not a solution in itself to such problems. There is inherent belief that it may make a difference in controlling it. However, in relation to computer crimes, it may not be stated with such certainty. Proliferation of computer related illegal and unethical activities in future may compel criminologists to consider any unethical conduct with the computer as a crime.

Criminology is on trial, not only from a legal and a definitional perspective, but also from the perspective of explanations it offers for crime as a phenomenon. Traditionally, crime has been attributed to physical, social, psychological and economic factors. More specifically to poverty, unemployment and disadvantaged persons. Those who indulge in computer crimes are not from these. Computer criminals are unlike the traditional

crimes in India. It cuts across all class and caste barriers. In this, it poses a challenge to criminologists.

Successful identification, charging, prosecution and convicting will not suffice. The existing treatment strategies, both imprisonment and community corrections are unsuitable for the computer criminals. The same problem arises with the preventive programmes that have been traditionally adapted. Most of the computer criminals are highly educated, intelligent and have competent vocational skills. Therefore, present and future criminology needs to aggressively address these and other complex issues related to computer crimes. It is likely that future criminology will address more ethical issues rather than confine itself to legal ones only.

EJ. Lloyd (1990) discusses several cases relating to computer crimes in the United Kingdom, which were prior to the enactment of the Computer Misuse Act, 1990. The legal response to computer related crimes were known as computer abuse and dealt with under the existing legal provisions. They were instances which fell within the province of existing offences, which then had been applied to the protection of interest to the physical or tangible property rather than computer data; it was perceived that the victims of such instances could seek redressal under the existing civil laws.

---

19 Lloyd, Ian; "Computer Crime" (P.163-177) Computer Law-Edited By Chris Reed; (1990)
He further categorizes computer crime under three broad classes; the classification being dependent upon the role played by the computer. Firstly, the computer may serve as a means by which a crime is committed; Secondly, the computer may provide an environment within which the criminal conduct may occur; and lastly, the computer itself may be the victim of the criminal conduct. He has suggested the evolution of laws around this categorization, which were to be the basis of the laws relating to cyber crime in the United Kingdom.

Fl. Rowland and Macdonald (1990) also trace the development of the British Law, The Computer Misuse Act 1990. The term “Computer Crime” itself leads to some controversy. Tapper [(1987) Criminal Law Rev 4], describes the phrase ‘ungrammatical and inelegant’. Other writers are rather more dismissive of any perceived semantic difficulties: ‘Clearly it is easy to argue over a definition of computer crime. Such an argument seems fruitless and will not be engaged here (Encyclopedia of Information Technology Law, Volume II, Para 12.03; Sweet and Maxwell). They are for the retention of this term because it serves as a useful umbrella under which to address a range of quiet new and difficult Criminal Law problems.

Rowland and Macdonald are of the opinion that the origin of the phenomenon of computer crimes begin with computer fraud and hence,
studies must begin here. They cite R V Thompson (1984) 1 WLR 962 at 967 as the difficulties faced by the conventional laws to deal with fraud, particularly transnational computer fraud. They also cite another judgment pronounced by Lord Lane CJ in R v Gold and Schifreen (1987) QB 1116 at 1124, that the attempts to prosecute the accused under the existing laws was untenable and the fact that the dishonest conduct of the appellants conduct amounted to dishonesty, but gaining access to information stored within a computer system and copy the data stored within, and use it for personal gain, amounted to illegal; behaviour, was not present in the language used in the Act. The judgment ends with the finding that there is no criminality in the conduct of the appellants. If the thought arose to make such actions a criminal offence, it is a matter for the Legislature rather than the Courts.

G: According to Bell,21 Criminals have always exploited the technological advancements made by the mankind. The advent of firearms, the telephone, automobiles was used in the past. Along with these, the widespread use of computers in society has lead to computer related crimes.

---

His study concentrated on advancement of computer technology, which resulted in an increase of use of computers in committing crimes. He also studies ways and means of prosecuting computer related crimes.

H]. According to Barry K. and Rider A.K.22, Some have argued that organized crime is a problem of the last quarter of the XX Century and in the case of most states is a new phenomenon of course; so much depends upon what is organised crime. Groups against the law are nothing new. Nor is it novel that the primary motivation of such enterprises is - economic gain-spurred only by ‘plain old-fashioned’ greed and corruption. Banditry, smuggling, racketeering and piracy were just as much as a problem for the proctors and vigils of ancient Rome and they are for the Halian authorities. What has changed is the criminal’s ability to operate beyond the reach of the domestic legal system and, therefore, be able to conduct an enterprise in crime that in net goes amenable to the traditional criminal justice and its agents. Of course, in truth, thinking criminals have always sought to place themselves beyond the impact of Information Technology on organised crime.

The above study has focused on the use of technology in organised crime.

---

I]. According to Kern Alexander Jr., and Robert Munro\textsuperscript{23}, Advancing technologies have improved the ability of financial institutions and their users to conduct Cyber Commerce. Improved technology however, as also provided an opportunity for criminals and fraudsters to use computer software systems to transfer their illicit gains and thereby sustain their criminal enterprises. Cyber commerce depends on rapid, anonymous and unsupervised transactions. Such a system is extremely vulnerable to criminals seeking to launder money on the internet. In a system where there are millions or transactions unsupervised by internet service providers and authorities, electronic money laundering and other crimes that may be committed through the use of technology, has made the financial institutions vulnerable.

The above study is concentrated on the trends of money laundering using the legitimate banking software and internet resources. It also focuses on the vulnerability of the financial institutions to prevent and detect these.

J]. According to Richard E. Overill,\textsuperscript{24} in this article, the historical development of computer crime is traced and analyzed. Some of the major examples of the phenomenon are examined with particular reference to financial and commercial information systems and institutions. The varied


motivators of the computer criminals are also considered. Finally, some lessons for today's financial institutions and commercial IT communities are offered. The above trends are concentrated on the trends of computer crimes committed by criminals are also studied.

K]. In the opinion of Sameer Hinduja, many traditional crimes are now being aided or abetted through the use of computers and networks, and wrong doing previously never imagined, has surfaced because of the incredible capabilities of the information systems. Computer crime are requiring Law Enforcement Departments in general and Criminal Investigators in particular to tailor an increasing amount of their efforts towards successfully identifying, apprehending and assisting in the successful prosecution of their perpetrators. This study has summarised the key research findings in the area of traditional American Criminal Investigation. Similarities and differences between traditional and computer crime investigations are then presented and consequent implications are then discussed. Pragmatic suggestions as to how American Computer Crime Investigative Taskforce, can most competently fulfill their intended objectives are given in conclusion, via an hypothetical example of a specialized unit. It is hoped that past knowledge can be assimilated with current observations of computer related criminality, to inform and guide the science of police investigations in the future. This study has focused on

---

the existing methods of criminal investigations of cyber crimes in the United States.

2.2: LITERATURE ABOUT CRIMINOLOGY

The theories of criminology which the researcher has referred to are

1. Techniques of Neutralization.
2. Rational Choice Theory.
3. Routine Activities Theory.
4. Space Transition Theory.

Techniques of Neutralization

In the 1960s David Matza, and his associate Gresham Sykes, developed a different perspective on social control which explains why some delinquents drift in and out of delinquency. Neutralization Theory, or Drift theory as it is often called, proposed that juveniles sense a moral obligation to be bound by the law. Such a bind between a person and the law remains in place most of the time, they argue. When it is not in place, delinquents will drift. According to Sykes and Matza, delinquents hold values, beliefs, and attitudes very similar to those of law-abiding citizens. In fact, they feel obligated to be bound by law. Then, if bound by law, how can they justify their delinquent activities? The answer is that they learn "techniques" which enable them to "neutralize" such values and attitudes temporarily and thus drift back and forth between legitimate and illegitimate
behaviors. They maintain that at times delinquents participate in conventional activities and shun such activity while engaging in criminal acts. Such a theory proposes that delinquents disregard controlling influences of rules and values and use these techniques of neutralization to "weaken" the hold society places over them. In other words, these techniques act as defense mechanisms that release the delinquent from the constraints associated with moral order. In *Delinquency and Drift* (1964), David Matza suggested that people live their lives on a continuum somewhere between total freedom and total restraint. The process by which a person moves from one extreme of behavior to another extreme is called drift, and this is the very foundation of his theory. Along with Sykes, Matza rejected the notion that subcultures of delinquency maintain an independent set of values than the dominant culture. They hold that delinquents actually do appreciate culturally held goals and expectations of the middle-class, but feel that engaging in such behavior would be frowned upon by their peers. Such beliefs remain almost unconscious, or subterranean, because delinquents fear expressing such beliefs to peers.

Techniques of Neutralization suggest that delinquents develop a special set of justifications for their behavior when such behavior violates social norms. Such techniques allow delinquents to neutralize and temporarily suspend their commitment to societal values, providing them with the freedom to commit delinquent acts. Sykes and Matza's theoretical model is based on the following four observations.
1. Delinquents express guilt over their illegal acts.

2. Delinquents frequently respect and admire honest, law-abiding individuals.

3. A line is drawn between those whom they can victimize and those they cannot.

4. Delinquents are not immune to the demands of conformity.

Thus, Sykes and Matza propose the five Techniques of Neutralization.

Denial of responsibility. Delinquent will propose that he/she is a victim of circumstance and that he/she is pushed or pulled into situations beyond his/her control. ("It wasn't my fault!")

**Denial of injury.** Delinquent supposes that his/her acts really do not cause any harm, or that the victim can afford the loss or damage. ("Why is everyone making a big deal about it; they have money!")

**Denial of the victim.** Delinquent views the act as not being wrong, that the victim deserves the injury, or that there is no real victim. ("They had it coming to them!")

**Condemnation of the condemners.** Condemners are seen as hypocrites, or are reacting out of personal spite, thus they shift the blame to others, being able to repress the feeling that their acts are wrong. ("They probably did worse things in their day!")
Appeal to higher loyalties. The rules of society often take a back seat to the demands and loyalty to important others. ("My friends depended on me, what was I going to do?!")

Sykes and Matza further argued that these neutralizations are available not just to delinquents but they can be found throughout society.

Attempts have been made over the years to verify the assumptions made by Neutralization Theory, and the results have, thus far, been inconclusive. Studies have indicated that delinquents approve of social values, while others do not. Other studies indicate that delinquents approve of criminal behavior, while others seem to oppose it. Neutralization Theory, however, remains an important contribution to the field of crime and delinquency. Social bond theorist, Travis Hirschi, asked an important question: do delinquents neutralize law-violating behavior before or after they commit an act? Neutralization theory loses its credibility as a theory which explains the cause of delinquency if juveniles use techniques of neutralization before the commission of a delinquent deed and therefore becomes a theory which simply describes reactions that juveniles incur due to their misdeeds. The theory does fail on the account that it doesn't clearly distinguish why some youths drift into delinquency and others do not. The theory remains too abstract and vague to be of any practical use unless we understand why drift occurs, critics have argued.26

26 Sykes and Matza's Techniques of Neutralization (Drift Theory)
http://people.ne.mediaone.net/dianedemelo/crime/sykes_matza.html (1 of 2) [10/1/2001 ]
Rational Choice Theory

In criminology, the Rational Choice Theory adopts a utilitarian belief that man is a reasoning actor who weighs means and ends, costs and benefits, and makes a rational choice.

In democratic countries, the broad appeal of both liberal and rationalist philosophies has steadily lead to the strengthening in importance of the western hemisphere's overall ideological premise from the point of view of defending the ideas of John Stuart Mill, the founder of utilitarianism.

Rational choice theory has sprung from older and more experimental collections of hypothesis surrounding what have been essentially, the empirical findings from many scientific investigations into the workings of human nature. The conceiving and semblance of these social models which are hugely applicable to the methodology expressed through the function of microeconomics within society are also similarly placed to demonstrate that a sizable amount of data is collated using behavioural techniques which are tweaked and made adjustable in order to ensure compatibly with the spontaneous motivational drives displayed by the consumer.

The theory is related to earlier drift theory (Matza: 1964) where people use the techniques of neutralisation to drift in and out of delinquent behaviour, and the Systematic Crime Theory (an aspect of Social Disorganisation Theory developed by the Chicago School), where Edwin Sutherland proposed that the failure of families and extended kin groups expands the realm of relationships no longer
controlled by the community, and undermines governmental controls. This leads to persistent "systematic" crime and delinquency. He also believed that such disorganisation causes and reinforces the cultural traditions and cultural conflicts that support antisocial activity. The systematic quality of the behaviour was a reference to repetitive, patterned or organised offending as opposed to random events. He depicted the law-abiding culture as dominant and more extensive than alternative criminogenic cultural views and capable of overcoming systematic crime if organised for that purpose (1939: 8).27

ROUTINE ACTIVITY THEORY

Routine Activity Theory (RAT) is one of the main theories of "environmental criminology". It was developed by criminologists Lawrence Cohen and Marcus Felson, who have worked for a number of years on crime prevention theory. RAT states that for a predatory crime to occur, 3 elements must be present when any crime is committed. RAT incorporates the crime triangle, sometimes referred to as the "problem analysis triangle" (PAT).

Features

Routine Activity Theory states that when a crime occurs, 3 things happen at the same time and in the same space:

- a suitable target is available
- there is the lack of a suitable guardian to prevent the crime from happening

---

27 William III, Frank. P; McShane, Marlyn. D.; "Criminogy Theory-Selected Classic Readings (P.131-240); Anderson Publishing Company; Cincinnati, Ohio; (1993)
• a likely and motivated offender is present.

A Suitable Target

The first condition for crime is that a suitable target must be available. The word target has been chosen carefully, rather than other words such as victim.

There are 3 major categories of target. A target can either be:

• a person
• an object
• a place.

There are plenty of potential targets around us, but not all of them are suitable. Two acronyms are sometimes used to describe suitable targets:

1. **VIVA**: Value, Inertia, Visibility, Access

Targets may also be repeat targets.

No matter how suitable a target is, an offence will not occur unless a capable guardian is absent and a likely offender is present.

Absence of a Capable Guardian

The second condition is that a capable guardian whose presence would discourage a crime from taking place must be absent.

A capable guardian has a 'human element', that is usually a person that by their mere presence would deter potential offenders from perpetrating an act. A capable guardian could also be CCTV, providing that someone is monitoring it at the other end of the camera.
Some examples of capable guardians:

- Police patrols
- Security guards
- Neighborhood Watch schemes
- Door staff
- Vigilant staff and co-workers
- Friends
- Neighbors
- Close Circuit Television (CCTV) systems

Some of the guardians are formal and deliberate, like security guards; some are informal and inadvertent, such as neighbours.

It is also possible for a guardian to be present, but ineffective. For example a CCTV camera is not a capable guardian if it is set up or sited wrongly. Staff might be present in a shop, but may not have sufficient training or awareness to be an effective deterrent.

**Likely Offenders**

When a suitable target is unprotected by a capable guardian there is a chance that a crime will take place. The final element in this picture is that a likely offender has to be present.

Routine Activities Theory looks at crime from an offender’s point of view. A crime will only be committed if a likely offender thinks that a target is suitable and a capable guardian is absent. It is their assessment of a situation that determines whether a crime will take place.

**Crime Triangle (also called Problem Analysis Triangle PAT)**

RAT introduces an important tool in crime analysis, the crime triangle (which has also been called the problem analysis triangle (PAT)). In the past the
Crime Reduction Centre has presented these 2 triangles separately with PAT being used in the analysis of a crime problem (victim, location, offender) and RAT use to develop the interventions (target/victim, location and absence of a capable guardian). The latest formulation of the crime triangle sees a combination of the 2 helping to think about responses as well as analysis.

Routine Activities approach is important to crime prevention and to the changing of conditions and circumstances in which crime is committed. One measure of situational crime prevention is target hardening. Target hardening makes it more difficult for offenders to carry out crimes on specific targets. The use of locked doors, windows, alarm systems, watch dogs, and community crime watch programs are all examples of target hardening--making it harder to become a victim of crime.  

---

SPACE TRANSITION THEORY

The 'Space Transition Theory' developed by Jaishankar explain the causation of crimes in the cyberspace. The general theoretical explanations of crime were found to be inadequate as an overall explanation for the phenomenon of cyber crimes (Jaishankar 2008). "Space Transition Theory" is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace (Jaishankar 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another. The postulates of the theory are:

1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.

2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime
3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.

4. Intermittent ventures of offenders into the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.

(b) Associates of physical space are likely to unite to commit crime in cyberspace.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.\textsuperscript{29}

The above theories of criminology are used in this research to evolve the hypothesis and formulate conclusions, based on the data collected and analysed.