Chapter 1

CYBER CRIME: A CONCEPTUAL AND THEORETICAL FRAMEWORK
1.1 Introduction

First coined by William Gibson\textsuperscript{1} in his 1984 novel ‘Neuromancer’, the term ‘Cyberspace’ is a popular descriptor of the virtual environment in which activity of internet takes place. The term cyberspace has become so common that it seems to dominate the thinking of people who consciously or subconsciously feel that they are entering a place which has new meanings, dimensions and purposes. Internet has created new public spaces and communities. These spaces and communities are known as virtual because they are no longer linked with place or time. However, they have common interests in social, cultural and psychological realms. They are based on ‘Computer-mediated-Communication’ (CMC) and ‘Human –Computer Interaction’ (HCI). This has led to the emergence of Network Society. The Primary condition to be a part of virtual community is a network connection and a desire to be a part of a wider community called as Virtual Community. Virtual Community is a combination of individuality and sociability in modern Network Society\textsuperscript{2}

Reflecting social anxieties about this surprisingly new phenomenon, the early studies which attracted the most attention were those that focused on pathological internet use and “addiction” Young (1998)\textsuperscript{3}, but as
sociology delved deeper into cyberspace, some very basic questions became apparent. Do traditional concepts and theories suffice in our understanding of online behaviour? Do we have to modify these theories? Do we need to develop new ones? These questions arise out of the recognition that cyber space as a sociological realm is quite different from face to face environment. Geographical boundaries are transcended. Everything is recordable and no boundaries of “privacy” exist. Social interactions can be synchronous, asynchronous, or something in between. Under complete anonymity, people become more disinherited than usual, or they might experiment with different identities. Sensory experience is expanded to multimedia experiences with highly creative fantasies. All these features of online space are characteristic of contemporary society i.e. network society.

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time but the basic crime ideas remain same. The significant change in modern time is on increase in personal computing power in a globalized communication network. The networked technology has become more than simply a force multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed. Internet is a set of social
practices; it is the kind of purpose to which we put the internet that creates the possibility of criminal and deviant activities. The internet provides the means to link up the many and diverse networks already in existence. Since commercialization of the internet during the mid 1990s, it has grown manifold. Even though majority of worldwide total internet connections are located in developed countries, the fact is that these are growing at a very fast rate in developing countries too. An Unequal access also follows along existing lines of social exclusion within individual countries and factors such as employment, income, education, ethnic disability are reflected in the patterns of internet use. Castells (2002)⁴. These inequalities point out the social characteristics behind the emergence of cybercrime and cybercriminals. Thomas and Loader, 2000⁵ conceptualize cybercrime as those Computer – Mediated-Activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. This definition reflects an important difference between crime (acts explicitly prohibited by law and hence illegal) and deviance (acts that reach informal social norms and rules, hence considered undesirable or objectionable). However it is worthwhile that crime and deviance cannot always be strictly separated in criminology. The boundaries between the criminal and deviant are socially negotiated and have become a recurrent feature of contemporary developments around the internet. Some
criminologists argue that cybercrime is not a new type of crime but is same as non virtual crime; it just uses new tools and techniques, while some others say that cybercrime is radically different and focuses on social structural features of the environment.

1.2 Cybercrime: A Conceptual Perspective

Theorists of the internet agree that cyberspace makes possible near and instant interactions between individuals who are spatially distant, which creates possibility for new forms of association which in turn gives rise to cyber crime and cyber deviance. Cyber crime, in simple terms, is a crime that is facilitated or committed using a computer, network or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. It can take place on the computer alone, or in other virtual or non virtual locations. It is recognized that current legal definition of cyber crime varies drastically between jurisdictions. A practical definition of a cyber crime is offered by Kshetri (2010). According to him, “Cyber Crime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations”. Examples of cyber crime include denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber
terrorism, and cyber extortions. It is evident that organized criminal organizations use cyber crime extensively to collaborate and connect with their vast network which is spread across globe. The synergy between organized crime and the internet has thus increased the insecurity of the digital world.

1.3 Categories of Cyber crime

It is very important to note the various categories of cybercrime and to place specific offenses into those categories. Cybercrimes can be easily placed into two categories; Violent and Non-violent cyber crimes. Most of the cybercrimes are nonviolent offenses, because of the fact that interaction is without any physical contact. Some of the nonviolent cybercrimes are cyber trespass, cyber theft and cyber fraud. The following diagram shows categories of cyber crime with various types placed in it:
Cyber Crimes

1.3(a) Violent Cyber crimes

(i) Cyber Terrorism
(ii) Cyber Stalking
(iii) Pornography
(iv) Cyber bullying

1.3(b) Non Violent Cyber Crimes

(i) Cyber Theft
- Embezzlement
- Unlawful appropriation
- Corporate Espionage
- Plagiarism
- Piracy
- Identity Theft
(ii) Cyber fraud
(iii) Cyber tress pass
(iv) Destructive Cyber crimes
- Cyber Vandalism
- Viruses
(v) Other Non-Violent Cyber crimes
- Cyber Prostitution
- Online Gambling
- Online Trafficking
- Internet Drug Sales

Diagram 1.1
1.3(a) Violent Cyber Crimes

Violent Cyber Crimes are those crimes that pose a physical danger to some person or persons. They are further classified as follows:

(i) **Cyber Terrorism**

The upsurge in internet activities has also given rise to a new type of cybercrime known as ‘Cyber Terrorism’. As the word suggests, “Cyber Terrorism” is basically a convergence between cyberspace and terrorism. Conventional understandings of terrorism nevertheless denote a distinct form of criminal action, characterized by the marriage of violence and politics Crozier (1974). USA has taken the lead to make legal provisions to protect the nation’s computer systems against terrorism after September 11, 2001 attack in New York and Washington. Even the critical infrastructure of any country is at risk due to cyber attacks. The disastrous cyber terror threat assessments include: Loss of power through attacks, disruption of financial transactions, Crippling transport systems including air and rail.

Several advantages are foreseen by the terrorist groups for virtual attacks. The internet enables action at a distance. Another advantage (which has proved as disadvantageous for society) is that it requires limited financial and material resources and acts as a force multiplier. The anonymity over the internet is quite easy through the use of
proxies\textsuperscript{10} which make difficult to trace the point of origin of the attack. It has already been noted that one of the greatest challenges presented by cybercrime to enforcement machinery is the extent to which the internet environment affords perpetrators a degree of anonymity or disguise. Flemming and Stahl (2000)\textsuperscript{11}. Besides all this, absence of any centralized and coordinated regulation of the virtual environment also poses the biggest problem. In the year 1999 Ethnic Tamil Gurillas swamped SriLankan embassies with lakhs of electronic mail messages. Denning (1999)\textsuperscript{12}. Terrorists attack through cyberspace is not only rampant in USA, UK, Israel and Egypt but also in India and Pakistan which may be treated as cyber war or electronic war against society. In India Terrorists are motivated for hacking and defacements of websites. Anti Indian Crew (AIC), Pakistani Hackers Club (PHC) G- Force Pakistan, Pro-Pak Hackers are terrorists groups who are working with Al-Qaida and Bin Laden. Some of these groups are represented by a technical expert who hacked the website of Zee News. He also attacked the website of Indian Cyber Crime cell at Mumbai with co-associate and posted objectionable material on that website abusing the police and administration. On 10\textsuperscript{th} January, 2001, the Director of CBI told the Info Sec News that a number of cases of hacking of Indian sites are traced to Pakistan. In July 2000, there were 635 incidents of breaking Indian internet sites. Hackers group called G- force published the message
against India claiming Kashmir. They also had defaced and hacked several websites of Indian government, companies and scientific organizations. The instance of hijacking of Indian airlines flight to Kandhar in Afghanistan in December, 1999, is an instance of cyber terrorism in India. Terrorists communicated and controlled whole operation through email but it remained undetected. On 13\textsuperscript{th} December 2001, attack on the Indian Parliament was abuse of Information Technology. It was a cyber attack. More than 100 websites provide recipes for making RDX bombs to net users worldwide. Not only this, electronic mail system for communication is the most reliable way for terrorists and they have their own websites to express and publish their views. They spread communal and other hatred through these websites.

(ii) **Cyber Stalking**

It is a type of cyber crime in which an attacker harasses a victim by using electronic communication. In some cases, cyber stalking originates from a real world stalking and is carried over to the internet. Stalking is a problem that many people especially women, are familiar with in real life. This problem that occurs through the medium of internet, is known as ‘Cyber Stalking’ or ‘On-line Harassment’. Cyber stalking includes harassment, embarrassment and humiliation of the victim. Cyber stalking can also result in personal hurt offline. Cyber stalkers are
motivated by hate, anger, revenge, jealousy, obsession and mental illness. Delhi Police registered India’s First Case of Cyber stalking in the year 2003. A lady complained against an individual who was using her identity to chat over the Internet in the Delhi region for some days. He was chatting on the Net, using her name and giving her address and phone number and even used obscene language. Consequently, she received almost 40 calls in three days mostly at odd hours from far off places. The said calls created havoc in her personal life and hence she reported the matter. Finally, the IP addresses were traced and police arrested the culprit on the said complaint. A case was registered under section 509, of the Indian Penal Code (IPC).

(iii) **Pornography**

Internet is easily accessed on computer, pocket PC, wireless, mobile phone, etc. In the late 1970s and early 1980s, programmers were zealously developing software enabling images that are transmitted, recomposed and viewed through Usenet systems. By 1996, of the ten most popular Usenet groups, five were sexually oriented and one (atl.Sex.Net) attracted some 5,00,000 readers every day. Lane (2001)\(^\text{14}\). To a much surprise pornography is the first successful e-commerce product. An important mention here is about a case which was filed in the Juvenile Court, Delhi on the charge of cyber pornography. Some jurist
says this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court. A student of a reputed school, New Delhi was arrested by Delhi police in year 2001, April because he created a porn website as revenge of having being teased by classmates and teachers. He listed the names of his 12 schoolmate girls and teachers in sexually explicit manner. He was charged under section 67 of the Information Technology Act 2000 and section 292,293, 294 of the Indian penal code and the indecent representation of Women act. Another case is of internet chat room in which a 30 year old man represented himself as a girl before a boy from year 2002 to 2004. The boy ran away from his home to meet this so called girl at Mumbai and discovered the truth. The accused men sexually abused the victim, stole money from him and beat him up. This was the result of chat room friendship which caused homosexuality which is prohibited under section 377 of the Indian Penal Code, 1860. In 2005 February, many girls and boys were found in Meerut Cyber café in indecent position. They were subsequently arrested for surfing porn websites. Another important issue which has raised public concern is the fear of minors being exposed (either wittingly or unwittingly) to sexually explicit, adult oriented content online. It has been noted that even the most seemingly innocuous web reaches often return results containing content deemed unsuitable for children .Zimmer and Hunter(1999)\textsuperscript{15}. Not only this is a
matter of concern, but the circulation of sexual images of minors on the internet is provoking revulsion among the overwhelming majority in society. The greatest danger is that children are inevitably abused in the production of such images and the children all over the world face the risk from someone or others who could seek them for sexual gratification.

(iv) **Cyber Bullying**

Cyber bullying is an extension of physical bullying. It has two forms; Overt and Covert. Overt bullying is physical aggression and includes beating, kicking and sexual touching. Overt bullying is often accompanied by Covert bullying in which victims are excluded from friends group, stalked, gossiped about, verbally harassed and threatened. Cyber bullying is carried by adolescents through Internet. As more and more youth are using the internet for interpersonal relationships, the risk of being bullied is increasing. It leads to depression, anger and sometimes even suicide.

1.3(b) **Non Violent Cyber Crimes**

Non violent cyber crimes do not cause any physical damage to persons; instead they cause financial loss, psychological disorders and social harm. They are further classified as follows:
(i) **Cyber Theft**

Cyber Theft is a way of using a computer and Internet to steal money or information. This is also the most popular cyber crime because the ability to steal from a distance reduces the risk of detection. Cyber Theft includes:

- **Cyber Embezzlement**- Online embezzlement means misuse or alteration of data by an employee of a company who has legitimate access to the company’s computerized system and network. Example- an employee misusing the company’s computerized payroll system in such a way that he is paid extra.

- **Unlawful Appropriation** wherein an individual gains access from outside the organization to transfer funds and modify documents in such a manner that it gives him legitimate right to property he doesn’t own. Unlawful appropriation, differs from embezzlement as the offender is not interested with the valuables but gains access and transfers funds or modifies some information.

- **Corporate Espionage**- In this crime, an individual from inside/outside the company uses the network and steals marketing strategies, trade secrets, financial data, client lists etc in order to gain a competitive advantage. In corporate or industrial espionage,
the person uses the company’s network to steal trade secrets, financial data, confidential client lists, marketing strategies or any other information to gain a competitive edge.

- **Plagiarism** is to steal someone else’s original writing and call it as its own. This form of crime is increasing everywhere as more and more people have access to computers and internet.

- **Piracy** is an unauthorized copying of copyrighted software, video, music, books, etc which causes loss of revenue to the owner. Cyber piracy is the appropriation of new forms of intellectual property, in which the computer programme, expressed in the form of a digital code, generates through a computer system ‘virtual products’ such as images, music, office aids or interactive experiences. When cyberspace and intellectual property laws interact they become a powerful force, especially in present day society where economic profit is quite important.

- **Identity Theft** - In this victim’s personal information is stolen by the criminal to commit financial frauds.

(ii) **Cyber Fraud**

Another form of cybercrime which has a firm grip on society is cyber fraud and scams online. But, the problem with this is the lack of systematic and official data. Internet Crime Complain Centre (ICCC)\(^{16}\) is
the only source available whose primary role is to receive public reports of cybercrime and refer them to the relevant criminal justice agencies for action. Hani Durzy, an eBay spokesperson in USA, claims that frauds ascent for only 0.01% of transactions undertaken using the site yet this would amount to 3000 frauds per day, given that more than 30 million auctions take place on eBay daily Cha (2005)\textsuperscript{17}. The fact is that a growing number of internet auction sites provide thieves a global market through which they sell stolen items to unsuspecting customers. For example, a group of motorcycle thieves in Austin and Texas, who dismantled various bikes and sold them online as spare parts for $15000. Another form of reported fraud is non delivery of items for which the victims have already paid. It can also include product in authenticity and misrepresentation of the condition of the item. In cases of shill hiding, the seller places false bids by either using multiple fake identities or aliases to place bids on their own items or by arranging for associates to place bids for the items with no intention of actually purchasing them. Thereafter it becomes impossible for the legitimate bidders to detect whether or not others are genuine buyers or shills. In recent years Phishing and Spoofing frauds have increased. Phishing proceeds through the mass distribution of emails that purport to originate from banks, credit card companies and e-sellers. These mails request for providing personal and other details in order to update their account. The
fraudsters thus gain access to the password and other security and authentication information of users, which can then be used to hack bank accounts or steal through credit cards. According to the Anti–Phishing Working Group (APWG), there were over 2500 such sites reported on the internet in January 2005 alone, a 100% increase in the number in comparison to previous year (APWG,2005)\textsuperscript{18}.

Internet offers valuable opportunity to fraudsters to disguise themselves and their identities. These fraudsters also change personal attributes such as age, gender, ethnic group, country of residence and so on. Even though the fraud is detected, identifying the culprit is very difficult. Victims of online frauds may be reluctant to report their victimization due to the following reasons; Relatively small amount of money involved does not make pursuing the matter worthwhile, embarrassment in reporting a fraud, ignorance about reporting the offence to the concerned authority, likelihood that no results will ensue as the fraudster is located in another country.

In India, the situation is no more different but rather more uncomfortable because companies are reluctant to lodge complaints about cyber fraud. They remain silent on such issues to protect their reputation in international market in an era of liberalization and globalization. Not a day passes by when a cyber fraud is not perpetrated in our country. The
magnitude of this is increasing by leaps and bounds. An individual, who was the owner of the website InfoTech Pvt. Ltd started his data conversion business in 1997 to give data entry works, to provide service for data entry, medical transcription, management and e-book etc. In January 2002, he fraudulently received Rs. 2.5 lakh non-refundable deposits from each of his clients giving false promise to give data entry work. He was arrested from Secundrabad on the charge of cyber fraud i.e. about Rs. 20 crore data conversion fraud. The Central Crime Station (CCS) investigators reported that six more cases have been registered under cyber fraud and police have identified at least 20 fake data conversion companies after this incident. This depicts the fact that technical experts are faced by culprits who use optimal technical assistance for committing crimes. One of the most pressing concerns for the policing of online fraud is the lack of specialized expertise and training. Resources need to be made available for the recruitment and retention of staff with necessary technical skills. Computer generated frauds have gained a wide attention as internet has become popular for commercial activity.

(iii) Cyber Trespass (Hacking)

In the case of cyber trespass a computer or network is accessed by the offender without authorization, but may not misuse it. For example, a
teenage hacker hacks a network just to prove himself to peers or takes it as a challenge. These trespassers enjoy reading emails of others but they don’t use any information they find. However, cyber trespass is a crime in majority of countries. Cyber crime causes more harm to society than traditional crimes. Hacking attack on AIMS, World Trade Centre, Bhaba Atomic Research Centre, RBI etc are examples of cyber hacking, they caused more harm than traditional crimes. Hackers do so because of curiosity, a desire to learn, discover and to freely share what they had found with others, damaging those systems intentionally or otherwise.

Hackers are confident that they would not be caught because; Few victims are interested to lodge complaint, due to unspecified and undefined jurisdiction in cyber world, most of the victims are unable to identify the culprits, as it is difficult to identify and understand the unauthorized use which is criminal trespass under section 441 of the Indian Penal Code. Becker (1963) calls this a labeling process; a process by which categories of criminal deviant activity and identity are socially produced. Even hackers are labeled as such because criminal justice and other agents propagate, disseminate and utilize negative constructions of hacking.

In December 2001, Indian websites of AIIMs, the Atomic Energy Research Board, Delhi High Court Bar Association etc. were hacked.
Victims were busy developing their internal system rather than reporting to police because they wanted to avoid negative publicity. Government was also under the false sense of security about companies, netizens and websites. Hacking took new shape between India and Pakistan i.e. net war, by way of defacement on websites. In the year 2005, almost 114 Pakistani sites were hacked by Indian hackers and about 766 Indian sites were hacked by Pakistani hackers. According to Mr. Anubhab Kalia (2004) 20 “for every Pakistani site defaced by Indian hackers, the Pakistanis hacked 10 Indian sites. There is a constant game of gunmanship happening online”.

(iv) Destructive Cyber crimes

In destructive cybercrimes, network services are disrupted or data is damaged or destroyed, rather than stolen or misused. They are classified as:

- **Cyber vandalism** is a form of vandalism that includes defacement of a website and denial of service attacks.

- **Spread of New viruses** has seen an upsurge in recent years. Many viruses are linked to notable dates, such as Christmas, Valentines Day or April Fool’s day, as by doing so, virus writers and distributors feel that they have better chance of success. Some of the viruses (e.g. CodeRed, MyDoom), unknown to their owners
and/or users, ‘infect’ computers and are used to access personal
information illegally. For example, they can be used to gain
access to credit card numbers and then those numbers can be used
to purchase goods and services illegally.

(v) **Other non violent Cyber Crimes**

Many non violent cyber crimes include Online Prostitution, Gambling, illegal drug sales on Internet and Cyber laundering.

- **Cyber Prostitution:** It involves carrying out prostitution online through various advertisements on sites.

- **Internet Gambling:** It denotes customers who use credit cards online to place bets in virtual casinos.

- **Internet drug sales:** Online pharmacies sale drugs to customers who are unable to purchase it from public or private dealers.

- **Cyber laundering:** It means using the net to hide the illegal money. Online banking offers opportunity to criminals who open accounts in an offshore bank and transfers funds electronically.

Having given the conceptual framework and classification of cyber crimes, it becomes imperative to understand the factors and motivations behind the cyber crime.
1.4. Motivations and Effects of Cybercrime

A motivation involved in cyber crime depends on criminal’s intent and need.

Following are the common motives behind cyber crimes:

1) **Monetary Profit** – Like many offline crimes, cyber crimes are also motivated by the desire for financial gain.

2) **Political Motive** – Internet is used by extremist and radical groups for propaganda, to attack the websites and network of their opposite groups.

3) **Sexual Impulses** – Sexually deviant behaviour is illegal and is considered harmful. People view porn sites to fulfill their immoral desires and needs.

4) **Entertainment** – Many cyber crimes are done for fun and enjoyment unlike other cyber crimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both a means and an end.

5) **Emotional Motivators** – Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. Revenge is much better planned than anger and it could be more dangerous because cyber
criminal has more time to think and plan his tracks which often reduces the possibility of being caught.

Global connectivity can create havoc in a very short time frame, throughout the world. Its nature and particular features have posed a unique challenge for investigators because of the following reasons; Global reach, Anonymity, Fast speed with which crime can be committed, the transient nature of evidence, and the high costs involved in investigations.

The challenge for the law enforcement authorities are diverse and includes; Bridging multijurisdictional boundaries, retention of evidence, decoding of encryption (complex process), proving of identity, coordinating investigative activities, improving the reporting of internet crime, acquiring, developing and retaining specialist staff and policing which is a primary challenge. Today everyone in industrialized countries has access to computers and internet. Children learn to use PCs at an early age and people who don’t have computers use cybercafés and other public places. Thus, the importance of technology and networking cannot be undermined in any society which is progressive and dynamic.

A conceptual Framework is a structure of what has been learned to best explain the natural progression of a phenomenon under study, while theoretical framework is an explanation of the phenomenon. Theoretical
Framework consists of theories, principles and research findings which are closely related to the present study under investigation. It guides the researcher in the interpretation of results. The researcher has tried to develop a theoretical framework about cyber crime. Such a theoretical framework is vital to understand the cyber domain and technology that has deep rooted impact on global interactions.
1.5 Theoretical Framework

Diagram 1.2
1.5(a) Classical Sociological Theorists

Comte’s (1865)\(^1\) positive philosophy is his real contribution to social and political philosophy. For him Positivism is the last stage of intellectual development. Reason and objectivity is the basis of positivism of his philosophy. Comte gave more importance to analysis, experimentation and observation. According to him positivism is not only responsible, but inevitable for social reconstruction. It is essential for bringing a new society and new social order. Even though Comte did not talk about crime, but reason which is the basis of positivism has a strong foothold in conduction of crime. Many of the crimes are organized and planned reasonably so that least of the suspect is left behind. Criminals use their brains as much as intellectuals so that no footprints are left behind. They are objective and use reasoning and observation for criminal acts. Even cyber crime has a logical basis as it involves analysis, objectivity, technical knowledge, experimentation and observation. Comte also believes that social development is the outcome of the development of human mind. As human mind progresses, the society also develops and criminal tendencies and new types of crime emerge. Cyber crime is no exception to this development. It is in the final stage of development that man is least fearful about God or any abstract force which gives him a reason to commit crime and deviance.
Following the footsteps of Comte, many classical sociologists favoured a scientific approach to study society and social problems.

(i) Durkheim\{1893(1933)\}\textsuperscript{22} emphasizes the fact that as the society advances and industrialization progresses, division of labour not only becomes important but also inevitable. Division of Labour is associated with specialization of labour. It is with the help of division of labour that society becomes more efficient, which in turn results in social progress. Progress gives rise to many new vocations and new inventions. Since there is division of labour and specialization, everyone does only a limited job with the result that there is dependence on others who are specialized in their own fields. Durkhiem gave the notion of social solidarity and identified its two major types – Mechanical and Organic. Mechanical solidarity is based on shared beliefs and sentiments while organic solidarity means the integration that result from specialization and interdependence. It is a consequence of moral and material density. Material density denotes a rise in population while moral density refers to the rise in interactions amongst people in society. The contemporary society has seen the emergence of organic solidarity which is an evolved form of mechanical society. While mechanical society is dominated by
repressive laws, the organic society is predominated by restitutive laws. The later type of society restores the status quo by using administrative machinery. New groups and interests develop and so do new criminals and crimes. Cyber crime is a feature of organic solidarity where heterogeneity and complexity occurs. According to Durkheim there is no society without crime but instead, every society has crime and is normal. In his view crime occurs when an individual diverge from the collective norms and exhibit a criminal character. Further, he views crime as a collective function which is important for reinforcing social norms and increasing consensus. Cyber crime is no doubt borderless and it occurs in abstraction, without any face-to-face interaction. It has brought together governments of various countries on a common front to make laws to fight against cyber crimes.

(ii) Weber (1991) introduced ‘rationalization’ to explain societies of west who have shifted from traditional orientation to rational and scientific orientation. Rationalization is a process which replaces traditional and subjective thinking with reason and objectivity. He believed that history has seen societies with traditional mode of thinking and modern society is rationalized. Even though rationalization results in technological advancement,
Weber feared that it would lead to dehumanized and alienated element. Rational society is based on social actions with “rationally pursued and calculated ends”, where “the end, the means, and the secondary results are rationally taken into account and weighed”. They involve an actor’s calculation of the best means of achieving a given end (example how to make maximum profit by online theft) or even a consideration of different end. Weber notes that the utility of each end is considered and there is a ranking of the utility associated with each end and therefore, ends having greater utility are pursued first in comparison to less important ends. All these features are suitably applicable for crime and cyber crime as well. Cyber crime can be committed for known as well as unknown persons. Cyber criminals know that it is easier for them to commit ‘e-fraud’ in comparison to committing fraud in physical space. They have calculated ends and means. They commit crime in such a manner that leaves negligible chances to be caught.

(iii) Marx’s\(\text{1932(1844)}\)\(^{24}\) concept of Alienation can be aptly used as a tool for understanding contemporary society. Technology has become a part and parcel of present society and Marx has referred to production as a technical process as it involves technology. Man
has attempted to gain control over nature by means of technology. Great success is achieved and man has obtained large degrees of control over nature, time and distance. However, the control and order exercised by technology seem to extend over man himself. It is as if man has lost control over his own instruments. It is the dynamics of technology because humans have engrossed themselves in this all powerful social fact. According to Marx, alienation renders Powerlessness. Indiscriminate use of modern technology has alienated man from himself and people around him. Man has himself become an object or material in the organization of modern technology leading to powerlessness; an aspect of new technological culture that has deprived man from face-to-face relations. Virtual world poses many challenges for the society. Even though many types of cyber crimes such as cyber bullying, cyber defamation and cyber blackmailing occur in virtual environment but they do have an effect in real life. However, it is very difficult to control these online crimes in physical world because of lack of adequate knowledge and expertise which is required to deal with online crime. This causes alienation in present generation who although is techno savvy and active on various social networking sites feel powerless to deal with cyber crimes.
(iv) **Pareto** *(1961)* states clearly that every individual performs both logical and Non-logical actions. In fact everyone tries to justify even non-logical actions as logical. He also believes that every social phenomenon has two aspects: one is reality and the other is its form. Whereas the former involves the actual insistence of the thing, and form is the way in which phenomenon presents itself to human mind. The former he calls objective and later as subjective aspect. He also believes that all actions of the individual have two aspects; one being the end and the other being means to an end. When means employed for achieving ends are correct, we call the action as logical otherwise they are non-logical. Similar is the case in technology, where many actions seen as logical by the actor (subjective) cannot be logical in reality (objective). For example Hackers view hacking as useful and profitable. The viewers of porn sites never call it as harmful. Nevertheless, cyber crime is a severe form of deviant behaviour but deviants justify it as logical and acceptable.

(v) In views of **Veblen** *(2003)* process of social change is more or less constant, and one change results in another change. Whole process of change cannot be resisted. For him social change indirectly reflects our technological advances and vice versa. The use of internet has established online communities which have
brought new kind of social relationships. Relationships on networking sites also turn real when people are seriously involved. It is through the use of technology that people learn more about worldly affairs. Use of mobiles and internet for instant communication have become commonplace. However, technology has also given rise to a new type of crime i.e. cyber crime. Online crime can be conducted from anywhere and at any time with a computer and a network connection. It leads to easy victimization. Pornography has degraded social and moral values of youngsters and even children.

(vi) **Tonnies(1991)** vividly mentions the concepts of Gemeinchaft and Gesselschaft. In Gemeinchaft (community) each person has some sort of relationship with others (without a choice), while in Gesselschaft (association) members enter into interaction according to their individual desires for achieving some specific purpose. Association has elements of self interest whereas community has the element of co-operation and interdependence. The emerging world society falls in the category of Gesellschaft where communication is virtual and individuals enter into relationship on their will for some specific motives. Such interactions occur on social networking sites where individuals
freely enter or leave a relation as per convenience. However, it has led to emergence of negative consequences such as cyber bullying, cyber defamation and cyber stalking.

(vii) In his essay, ‘On liberty’ John Stuart Mill (1859) elaborated the notion of state as Paternalistic. If Mill is correct in suggesting a need for a balance standard between the society and state, there emerges a series of complex issues and questions. If law is an instrument to preserve the “civilized community through imposing morals and virtues, then where is the means by which such assessment is made”. Such is the current situation with respect to the presence of sexually explicit material online in our society. It is very easy to find thousands of porn sites on internet which can be viewed, downloaded, transferred at fast pace without any legal or social restrictions. Government has not been able to implement ban on porn sites although law prohibits its viewing and downloading. The Law is present but it is difficult to be implemented in the cases of online crimes.

1.5(b) Modern Sociological Theorists

(i) Merton (1938) opines that gap between approved goals and the means creates strain. In contemporary society, success is primarily measured in terms of material achievements and social standing.
In a mixed shape of economy such as India, individuals have to choose their own path and work hard to earn living. This leads to competitive nature of careers and employment. Merton used anomie theory to apply specifically to deviant behaviour in various societies. In the contemporary society, success is probably rated a lot higher than virtue. His theory proposes that those individuals, who are underprivileged, may end up as taking honest and socially acceptable path to meet financial success and yet not end up as successful, as those who are not in the same position. This would lead them to question why they would take the honest path when they could be more successful through deviant behaviour. Cyber criminals come from a very diverse background. Those who are in higher schools or colleges are most likely to fit into these theories. They may see how they put a lot of hard work into their studies and development of skills and yet realize that it is unlikely that they could achieve the financial success. As a result they may see crime as a means to achieve enormous financial success. Any individual would see computer crime as a way and means to make large sums of illegitimate money.

Modernity recognizes the advantages of technology and sees risk as its inevitable feature. The point is how this risk can be
prevented, minimized or channeled. In classical modernity the ideal was equality while in contemporary modernity, the ideal is safety.

(ii) **Giddens (1991)** describes the modern world as a ‘Juggernaut’ which is a runaway engine of enormous power which, collectively as human beings, we can drive to some extent but which also threatens to rush out of control and which could render itself asunder”. Internet is a product of modern technology moving along through time and over physical space. Digital netizens are the agents who steer it in their directions. Distanciation i.e. close linkage between time and space is broken through net. In this sense, both time and space are devoid of content and have become pure forms. Thus, with modernization, time is standardized and the close linkage between time and space is disappearing. Relationship with those who are physically absent and increasingly distant are more and more likely. Time and space distanciation is important in modernity for several reasons; first it links local and global domain, second, modern world is able to mould the present, and third, such distanciation is a major prerequisite for the source of dynamism in modernity – i.e. ‘Disembedding’. Disembedding involves lifting out of social
relations from local levels of interaction. It has given rise to online relationships with those who are physically absent and increasingly distant. Social relations online are globalized and people do have friends from all over the world now. Friends are now made on the basis of common interests and goals. There are two types of disembedding mechanisms that play a key role in modern societies. First are symbolic tokens and second are expert systems. ‘Symbolic tokens’ are money, which allows for time space distanciation. We are able to engage in transactions with others who are widely separated. This has also give spurt to online frauds and hacking through which cyber criminals can make transactions from any part of the world at any time. The use of credit cards online exposes the user to the risk of identity misuse and eventual fraudulence. Second mechanism i.e. ‘Expert Systems’ involve professionals like lawyer, physicians and engineers; common things like cars, gadgets are also created and affected by Expert Systems. They provide guarantees (but not without risks) of performance across time and space. Personal Computers are always prone to viruses while using internet. Trust is very important in modern securities dominated by abstract systems. Online trust on someone with whom one is transacting or forming any relationship plays an important role but because of
lack of physical proximity, it becomes easier for an individual to break the relationship at his own will and at any time because he or she is not answerable to anyone. Cyber experts are limited in number because of the technical skills required in this field which are complicated and difficult to learn. Besides this, cyber crime is conducted from any part of the globe at any time by anyone.

Giddens talks about new and dangerous risks associated with modernity that always threatens our trust. Risk is global in intensity (cyber war). A wide range of public knows about risks we face and are also aware that expert systems have a limited role to play. The type of risks on the Internet has acquired varied forms such as e-fraud, e-theft, cyber bullying, stalking, cyber terrorism, pornography etc. These risks have far reaching social effects and have given us the feeling of a runaway juggernaut and fill us with ontological insecurity. Giddens also quotes several reasons about the negative effects of modernity like the design faults in the modern world and operator failure i.e. the problem is even not traceable to those who run the modern world. Abuse of technology and Internet can’t be controlled even by the administrators or Government.
(iii) Beck(1992) calls modern world as a ‘Risk Society’. The emerging new modernity and new technologies are associated with the risk society. The contemporary world has elements of both. Beck labels the new or better yet newly emerging form as reflexive modernity. A process of individualization has taken place in the west. The agents of modern era are free of structural constraints and as a result better able to reflexively create not only themselves but also the societies in which they live. Beck recognized a strange paradox in late modern society; risk is increasing due to technology and science rather than being abated by technological progress. It is not a world which is less prone to risk, but it is “world risk society’ as Beck explains. With magnitude of risk so great, that transcends both time and place, by becoming global in scope, the control of risk across is both impossible and meaningless. In the case of cyber crime one is unaware of the risk that can occur with a single click of mouse. Hacking, fraud and online schemes are some of the risks to which users are exposed. The ‘Information Society’ is thus creating risks for people thereby exhibiting a ‘Risk Society’. In the case of cyber risks, the weapons are software and knowledge, the environment in which the attack occurs is virtual; the possible attacker is unknown and is able to hide himself effectively.
Ritzer’s (2008) impetus is on the McDonaldization of society which represent a contemporary paradigm of formal rationality. He has given four dimensions of formal rationality:

- Efficiency i.e. the search for the best means to an end
- Predictability i.e. a world of no surprises
- Rational systems tend to emphasize quantity, rather than quality.
- Reliance on non human technologies

Thus Ritzer’s McDonaldization also applies to contemporary Cyber culture. The Information Society exhibits these features of modernity. So much information is loaded on the internet that one searches it for almost anything that he requires, whether it is sale or purchase of a commodity or a service, or even knowledge. It is highly predictable as one knows what to get and from which site. However, despite so much information being there on the internet, its authenticity remains a problem making quality of information on net an issue. Besides, information society relies on cyber environment which brings demystification and dehumanization with it.

The theories of modernity, thus see the Cyber society as a threat to the world system. Advancement of technology has given rise to associated
risks. Internet has definitely made life and work easier for people but has also exposed them to certain threats like online crimes.

1.5(c) Post modern Sociological Theorists

Post modern society has seen the dawn of sentiments and emotions. In the post modern era, the disadvantages of technology are recognized. While in modern society individualism was important, in post modern era, emphasis is on collectivity or groups.

(i) **Baudrillard (1984)** believes that there was a time when signs stood for something real, now they refer to little more than themselves. Distinction between what is real and what is fabricated is the cornerstone of the postmodern world. The distinction between signs and reality has imploded. It is characterized by such implosions as distinguished from explosions (of production system, of commodities, of technologies so on). Therefore, just as the modern world underwent the process of differentiation, the postmodern world can be seen as undergoing dedifferentiation, in a world where signs no longer have a natural meaning and are instead manufactured to take on symbolic meaning. According to Baudrillard ‘We live in the age of simulation’. It leads to “reproduction of objects or events”.

Software Piracy or the counterfeiting and distribution of products intended to pass for the original is done by illegal downloading. In photo morphing, a face can be morphed with someone else’s body; it is difficult to distinguish real from the duplicate. Baudrillard describes the post modern world as hyper reality. For Example, stealing the IP address or identity of another computer or to obtain access to the other computers on the network (Spoofing). Only a decade ago people had to trek down from one place to another for shopping. Now with a single click of mouse, these are available at one website from which we can order online. Shopping, banking, games, movies, entertainment are available online. In rationalizing these forms of re- enchantment, they are by definition disenchanted. Besides this e-commerce has given rise to a number of online cyber crimes. Identity theft and online transactions are examples, in which fraud can be conducted without physical circumstances.

(ii) Jameson(1991)\(^{34}\) recognizes that postmodernism is usually associated with a radical break. He describes this new form as a ‘cultural dominant’. According to Jameson four elements are basic to postmodern society:
• Postmodern society is characterized by superficiality and depthlessness. It truly depicts the use of internet and its activities. Emergence of social networking sites coincide with superficiality as the people who are connected through these networks lack the basic connection and sentiments which are required for long lasting relations. Jameson has used the term “simulacrum” in which one cannot distinguish between original and the copied.

• In Postmodern society, emotions or intensities have faded. It causes alienation and anomie. Jameson prefers to call it as ‘Intensities’. The new electronic media gives rise to post modern intensity. In cyberspace, humans lose their real self and dream about illusions in a virtual environment, which gives rise to unusual fantasies. Pornography is an example of such phenomenon.

• In Post modern society, there is a loss of historicity (pastiche) i.e. the past cannot be traced. All one has is the access to our texts or pictures. Even on the net one has to trust the information posted on it.

• Post modern society has impressions based on reproductive technologies, especially electronic media like TV, computer, and internet. The postmodern era gives birth to new and varied
cultural products than the explosive, expanding technologies of the modern era did. Cyber culture has produced a new type of culture in society which has both positive as well as negative aspects in it. For instance, Infringement of copyrights (Plagiarism) has increased on internet.

Thus we realize that post modernity is full of technical advancements but it carries within itself the forces of destruction. Cyber war is no exception to that. Developed as well as many developing countries rely on networks and servers for important services and activities. Economic strength definitely depends on these which are a pillar for good society too. Besides the theories of modernity and post modernity, many other theories need to be examined in the light of dynamic issues relating to cyber crime and social networking.

1.5(d) Other Theories

Some other theories also lend support to sociological theories discussed above. The following theories examine crime, deviant behaviour and transition of individuals from physical to virtual space and vice versa.

(i) Social Control Theory and Cybercrime

Social control refers to the effort of a group or society to regulate the behaviour of members in conformity with established norms. As a result, there are sanctions, or externally imposed constraints.
Some of these are informal sanctions and unofficial pressures to conform. When informal sanctions are not enough, formal sanctions come into play. These are officially imposed pressures to conform, such as fines or imprisonment. Through socialization and internalization of cultural norms and values, most people learn to pursue socially accepted means even without external sanctions. However, when this learning is faulty or incomplete, it results in deviance. Very little crime is committed by young children because they are constantly under adult supervision. Hirschi (1969)\textsuperscript{35}. However, adolescents and young people are relatively free from adult control. As a result, they experience less social control and of those who exhibit an underlying tendency to pursue short term immediate pleasure often engage in cyber crimes.

(ii) **Rational choice theory and cyber crime**

Cornish (2010)\textsuperscript{36} argue in his Rational choice theory that an individual decision to commit a crime is based on cost - benefit proportion. ‘Rationality’ means that an individual balances cost and benefit to arrive at action that maximizes personal benefit. Cyber stalkers commit a crime after weighing the prospective rewards against the potential risk. Stalking via the internet allows
the offender to do it from a relatively remote distance. The offence inflicts the same type of fear and harassment as in the case of victims who are in direct face-to-face situation with cyber stalkers. Rational choice theory is accepted by many people because it assumes that people act in a manner that is rational. It assumes that many of the cyber criminals are very talented and well educated, not necessarily in formal manner but they have an ability to think rationally. They attack the victims whom they believe would give them the greatest amount of financial gain with least chance of getting caught. The high tech cybercriminals are hardly caught because of the skill to cover their tracks and move through proxy servers so that they are undetected. They commit large fraudulent schemes and remain undetected online.
(iii) **Social learning Theory and Cyber crime**

Tarde (1903)\(^{37}\) explains the fact that individuals learn deviant behaviour and it is not biologically inherent. Tarde observes that there are four main requirements in which social learning occur; First individuals must have a close contact with those they are imitating which can be family members, close friends or teachers; second, individuals must engage in imitation of their superiors; third, is that they must understand their behaviour i.e. they need to know what the behaviour is like. The individual must be a role model to the person who is imitating the behavior. This theory takes into account the fact that the behaviour learnt could be negative as well as positive. Another important contributor to this theory is Bandura (1977)\(^{38}\) who asserts that most human behaviour is learned observationally and this information serves as a guide for action in future. Through the process of socialization an individual learns the norms of society .An individual with less experience views the more experienced person as a mentor. For example, the act of hacking is learnt in group interaction. Even photo morphing is learnt for fun which can be later used for defamation. Most of the cyber crimes are learnt as they involve the use of technology.
Criminologists have also used two primary theories to explain and analyze cyber crime; Aker’s (1998)\textsuperscript{39} Social learning theory and Gottfredson and Hirschi’s (1990)\textsuperscript{40} General theory of Crime. General theory is based on the premise that people with less self control are impulsive, insensitive, short sighted and risk takers, and are unable to resist the opportunity to offend. However, social learning theory proposes that crime is a learned behaviour stemming from peer association that leads to deviant attitude. Less self control is also linked to various forms of cyber crime including illegal download of music, piracy of movies, software piracy.

In terms of Akers associating with deviant peers is one of these strongest correlates of crime and provides deviant models for imitation. “Social learning theory has significant intrinsic value for understanding cyber crime because offenders must learn not only how to operate a highly technical piece of equipment but also specific procedures, programming and techniques for using the computer illegally”. Skinner and Fream (1927)\textsuperscript{41} Many studies have found consistent evidence that associating with deviant peers leads to a wide variety of cyber deviance.
Differential association and Cyber crime

This theory is most widely accepted theory in criminology. It was first proposed by Sutherland (1924)\textsuperscript{42}. It was originally created to explain rise in white collar crimes. The basic idea behind this theory is that criminal tendencies are learned in interaction with other deviant persons. It is through interaction with others that one engage in illegal acts. This theory could explain why normal law abiding individuals can turn into criminals or deviants depending on the circumstances that they may be put into. This theory consider social environment as a means to explain why some individuals engage in criminal behaviour. This is seen in poor socio-economic conditions which encourage disobedience of law and authority. The main premise of this theory is that criminal behaviour is learnt through social interactions. The groups created on various Social networking sites have framed their own norms and values for members. The new members have to accept these norms and values for online behaviour for close association. The norms of these groups often contradict with the norms of the society. Thus, through differential association with online deviants, individuals are socialized into a subculture of deviance.
(v) **Space Transition Theory**

“Space Transition Theory” is proposed by Jaishankar (2008). It explains the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and virtual space. Virtual space provides an individual with such space where he can express his feelings and even vent out his outrage against anyone. Cyber stalking and Cyber defamation are instances where offenders use online space because of its anonymity and widespread approach. It also argues that people behave differently when they move from one space to another. One of the important postulates of the theory is that ‘People 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’. Criminology views the emergence of cyberspace as a new locus of criminal activity and therefore, some new theories are needed to explain occurrence of cyber crime.

(v) **Network Theory**

This theory focuses on a wide range of micro to macro structures. Links occur at the large-scale, social-structural level as well as at micro level. While sociologists talks about ‘strong ties’, network
analyst talks about ‘weak ties’. Social networking sites preserve culture of maintaining weak ties. Weak ties prevent isolation and allow individuals to better integrate through Social networking sites. However, such integration also gives rise to deviant behaviour on social networking sites, because networks are transitive. If there is a tie between A and B and B and C, there is likely to be a tie between A and C. This link between A and C is weak and therefore could lead to some form of crime in cyber space like Identity theft and hacking of account. It is also observed by Rosenthat(2011) that networks have a dynamic quality with the structure of the system changing with shifting patterns of coalition and conflict.

1.6 Conclusion

The dynamic character of the contemporary society is regarded as a result of alarming alterations in social environment. Introduction of new cultural traits into society bring new social changes. Present society is dominated by a complex culture of networking and informationalism. The Information Technology Revolution has brought many changes in the social structure. People rely on technology for many needs. However, it is noted that abuse of technology has given rise to a new variant of crime
online i.e. cyber crime. Emergence of virtual society has associated risks with it. It is characterized by instant communication with anonymity, deception and disguise. Various theoretical explanations provide an answer to an in-depth curiosity about use and abuse of technology and how it has given rise to cyber crime. The classical theorists relate emergence of crime to the development of science and technology. The modern theorists, on the other hand discuss the effect of technology on contemporary society which they characterize as risk society, encouraging anomie, dehumanization and distanciation. The post modern theorists see the world as ‘hyper real’ and ‘virtual’, full of simulations and technological intensities facilitating spatial interactions and providing anonymity to cyber crime.

Cyber crime has serious impact on society in the form of psychological disorder, social disorganization and economic losses. Even though all people suffer from its ill effects, the most vulnerable group is adolescent and youth. It is because of the fact that 75% of the online population in Indian society is under the age of 35 (Report by Comscore, 2013)\(^46\). Adolescence is a time of questioning and experimentation, as teenagers frame their own identities. Present adolescents and youth are techno savvy and use
technology for various purposes. With more and more adolescent’s use of social networking sites, it becomes imperative to find out how networks are used by cyber criminals to lure young people. It is also necessary to find out whether these adolescents are only the victims of cyber crime or they are also potential offenders. The following chapter focuses on emergence of ‘Network Society’ and origin of Social networking sites. They are an inevitable part of contemporary society and it is essential to find out its pros and cons on society in general and on adolescents in particular.

Notes and References


8. Critical infrastructure (CI) is defined as ‘an infrastructure or asset, the incapacitation or destruction of which would have a debilitating impact on the national security or economic or social welfare of a nation (Dunn and Wigert, 2004)’ Dunn, M. and Wigert, I. (2004) *International CIIP Handbook: An Inventory and Analysis of Protection Policies in Fourteen Countries.* Pg 18, Swiss Federal Institute of Technology, Zurich.

9. A “force multiplier” is something that can increase the striking potential of a unit without increasing its personnel (White, 1991). White, J. (1991) *Terrorism : An Introduction,* (Pg 18)

   Pacific Grone, CA : Brooks/Cole

10. In *computer networks,* a **proxy server** is a **server** (a computer system or an application) that acts as an intermediary for requests from **clients** seeking resources from other servers. Proxies were invented to add structure and encapsulation to distributed systems.
Today, most proxies are web proxies, facilitating access to content on the World Wide Web.


13. Retrieved from [http://cyberlaws.net/cyberindia/2CYBER27.htm](http://cyberlaws.net/cyberindia/2CYBER27.htm)

14. Lane, F. (2001), *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age*, pg 66, Routledge, London. Lane has used the term usenet ;Usenet is distributed among a large, constantly changing conglomeration of servers that store and forward messages to one another in news feeds. Individual users may read messages from and post messages to a local server operated by a commercial usenet provider, which can be a university, employer, or their own server.


16. The purpose of Internet Crime Complaint Centre is to serve as a central hub to receive, develop, and refer criminal complaints regarding the rapidly expanding occurrences of cyber-crime. The IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations on the internet.


19. Becker, Howard (1963) Outsiders: Studies in the Sociology of Deviance, The Free Press, New York. Becker views deviance as the creation of social groups and not the quality of some act or behavior. Becker (1963) criticizes other theories of deviance for accepting the existence of deviance and by doing so, accept the values of the majority within the social group. According to Becker (1963), studying the act of the individual is unimportant because deviance is simply rule breaking behavior that is labeled deviant by persons in positions of power. The rule breaking behavior is constant, the labeling of the behavior varies (Becker 1963). Becker (1963) describes rules as the reflection of certain social norms held by the majority of a society, whether formal or informal. Enforced rules, the focus of Becker's (1963) approach, are applied differentially and usually facilitate certain favorable consequences for those who apply the label. In short, members of the rule-making society may label rule breaking behavior deviant depending on the degree of reaction over time (Becker 1963).


23. Mulligan, Martin (1932), Marx Economic and Philosophic Manuscripts of 1844 (Translated), Progress Publishers, Moscow.


25. Brette, Olivier. (2003) "Thorstein Veblen's Theory of Institutional Change: Beyond Technological Determinism". *European Journal of the History of Economic Thought, Vol 10*(3), 455–477. T. Veblen and Karl Marx have been called as determinists. Marx was economic determinist (because he believed that every social change came as a result of change in the means of production), Veblen believed that all social changes come as a result of changes in technology. Since he has laid stress on technology, Veblen has been called as “Techno – Logical Determinist”. Technology alone changes even the habits of the people on the one hand and material environments on the others. He also believed that material environments are constantly changing and every person has to adapt him to those changes. There are also changes in habits, thoughts and social relationship as a result of technological changes.

27. Mill, J.S. *On Liberty* (1859), Indianapolis: Library of Liberal Arts. From "On Liberty is a rational justification of the freedom of the individual in opposition to the claims of the state to impose unlimited control and is thus a defense of the rights of the individual against the state."


33. Jameson, Fredric (1991) *Postmodernism, Or the Cultural Logic of Late Capitalism*, Pg iv, Duke University Press. Durham, NC. As a cultural dominant, postmodernism is described as a “force field in which very different kinds of cultural impulses must make their way”


42. Jaishanksr ,k (2007), Establishing a Theory of Cyber Crime, Pg 7-9 *International Journal of Cyber Criminology, Vol 1 Issue 2*

43. In *social network theory*, social relationships are viewed in terms of *nodes* and *ties*. Nodes are the individual actors within the networks, and ties are the relationships between the actors. There can be many kinds of ties between the nodes.
