Journal of Advances and Scholarly Researches in Allied Education
Vol. 15, Issue No. 12, December-2018, ISSN 2230-7540

A Criminological Perspective on Cyber-crimes and Theories of Criminal Behaviour in Cyberspace

Rawat Singh*

Research Scholar, Department of Law, Maharaj Vinayak Global University, Jaipur

Abstract – Cyber world is the combination of computers and other communication convergence Technologies. No doubt the techno world has raised the job opportunities and the platforms to the youngsters to grow professionally as well as economically but at the same time it raises complex problems for traditional laws which are now to be applied in superhighway with new spectacle because these laws are not adequate in cyberspace always. Cyberspace has no specific location which is another problem in contemporary legal system. Cyber world is the world without specific boundaries where people with a keyboard and mouse by single click can visit whole world, can speak with any one they wish, can see any one they wish, even thousands of miles away, they can have online discussion with each other, exchange their views, sell and purchase things, access banking facilities, create information and exchange information online. For improving the legal system and to control the cyber-crimes it is necessary to seek the insight understanding of nature and behavior of the criminal. The theories of Criminology can help to make it possible to some extent to put hold on cyber-crimes.

Key Words – Cyber-crime, Cyber space, Information Technology, Internet, Electronic Communication, Theories of Criminology, Hacking, Cyber terrorism, Cyber stalking, Cyber theft, forgery, flowing of viruses and Cyber pornography.

----------X----------

INTRODUCTION

The term 'Cyber' is derived from the term 'Cybernetics' which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crime committed in cyberspace relating machines or devices or cyber technology related crimes are to be treated as cyber-crimes. Information technology and electronic commerce are widely used to facilitate crime or to commit crime. In wider sense cyber-crime is a crime on the internet which includes hacking, terrorism, fraud, illegal gambling, cyber stalking, cyber theft, forgery, flowing of viruses, cyber pornography.

"It is very essential to emphasize here that the world is not run by weapons any more, or energy, or money. It is run by ones and zeros… little bits of data… it is all electrons. There's a war out there, a world war. It's not about who has the most bullets. It is about who controls the information—what we see and hear, how we work, what we think. It's all about information".[1] The movie traced on Information Technology to commit theft in superhighway and information is the commodity to theft. Cyber-crimes are computer related as well as computer generated crimes. This is increasing every moment which is the cause of global tension. Therefore, law enforcing agencies must have detail knowledge and understanding about varying nature of cyber-crime. Though there is nothing new in the adoption of new technologies by criminals. In the era of liberalization and globalization we must recognize cyber-crime as significantly new phenomena which have political, social and economic impact worldwide. The global connectivity of internet makes possible for existing organized criminals to use sophisticated techniques to communicate between groups and within groups to support and develop networks for drugs trafficking, illegal arms trafficking, money laundering, smuggling, theft, fraud, pornography, terrorism and other cyber-crimes. Cyber-crime is a threat to national and international socio-economic, political and security system.[2] According to Loader B.D., a flexible communicable system designed to withstand attack by means of rerouting message has also proved difficult for governments to control. Sources of illegal activity often require advanced computer skills to be detected as a consequence of their anonymous character.[3]

Prof. S.T. Viswanathan has given three possible definitions of cyber-crimes and these are as follows:

(a) Any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer.

(b) Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

(c) Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.[4]

Multiple information can be transferred through internet world wide without much control and specific jurisdiction which is a factor for fast growth of cyber-crimes. It is very difficult task to define cyber-crime in the contemporary communication convergence era. A computer is a subject matter, it can be victim, it can be the facilitator and it can be the instrument of a crime. To discuss computer crime certain factors are to be identified such as how much data available in network, security measures available to protect those data and traffic in networking systems if any, connectivity whether easy and open or restricted with controlling measures. How much the system is accessible to people and whether general people are very keen to access the system, speedy growth and development of new Information Technology etc.

ELEMENTS OF CYBER-CRIME AND CRIMINAL LIABILITY

From the definition of crime it is clear that there are two elements of crime one is *mens rea* and another is *actus reus* with certain exceptions e.g., in conspiracy only *mens* rea is enough for imposing criminal liability. In crime against State e.g. false evidence, counterfeiting coin, white collar crime, etc. only *actus reus* are sufficient to impose criminal liability. The general principle of Criminal law is that no person is to be convicted of a crime unless it is proved beyond reasonable doubt by the prosecution that his conduct (act or omission) is prohibited by criminal law and he is liable for the same and also that he had a defined state of mind in relation to the crime commission. In other words *actus reus* unaccompanied with *mens rea* is not a crime.

Actus reus + *Mens rea* = Crime

Actus reus + *No Mens rea* = No Crime

No Actus reus + *Mens rea* = No Crime

This is the general principle that crime consists of two essential elements. There are five essential requirements for imposing criminal liability. These are: (1) human conduct; (2) circumstances; (3) consequences or result; (4) voluntariness; (5) foreseen or forcibility of result of his conduct in a circumstance which has causation of crime and there must be chain of causation and probable or natural consequence. Fifth one i.e., forcibility represent *mens rea* and other four requirements represent *actus reus*. So, it is not permissible and unjustified for the State to impose punishment where any one of the elements is absent; except exceptional cases. '*Actus reus'* is 'human conduct' or act which includes omission and under s. 33 of the Indian Penal Code 1860, act includes omission.

J.C. Smith and B. Hogan considered *actus reus* as such result of human conduct as the law seeks to prevent.[5] In rape the absence of consent on the part of the prosecutrix is an essential constituent of the *actus reus*. If this absence of consent is not proved by the prosecution then *actus reus* of the accused will also not prove and here the prosecution will fail. In this sense we can say sometimes *mens rea* is also the part of *actus reus*.

In case of cyber-crime it is very difficult to prove both elements of crime. Actus reus of cyber-crime is very dynamic and varied. For example when with a keyboard and mouse one start functioning with computer, when one is attempting to access information on others computer without the consent or approval of the authorized person, when is one attempting for hacking, flowing viruses, to commit cyber terrorism and actually caused those acts these are human conduct or *actus reus* in cyberspace which law seeks to prevent. These are again *actus reus* of cyber-crime. m*ens rea* is another essential element of cyber-crime. Smith & Hogan, state that till 12th century only for *actus reus* a man could be held liable for any injury without proof of *mens rea* or blameworthy state of mind. In modern Common Law this concept has been changed and now guilty mind or blameworthy state of mind is the essential element for crime commission and imposition of penalty. Words such as, recklessness, negligence, intention, knowingly, dishonestly, fraudulently etc. represents m*ens rea. mens rea* is not used and defined in the Indian Penal Code 1860 which is one of the major criminal laws in India. However, Indian Penal Code defines dishonestly, fraudulently etc. There must be on the part of the cyber-criminal foresight or m*ens rea* to commit crime. For example, while committing hacking, hackers have knowledge or intention of unauthorized access and thereby commission of crimes.

When any person knowing or intentionally accesses without the permission of the authority

(1) any information, computer, computer system or network therein and alters, damages, deletes destroys or uses those devises or executes any unlawful plan,

defrauds or wrongfully controls for financial gain and causes wrongful loss by this way;

(2) alters or copies any supporting documentation external or internal to it or adds, alters, damages, deletes, destroys any database software, programmes which reside or exist internal or external to a computer, computer system or computer network; or (3) disrupts or causes the disruption of computer services or denies or causes the denial of services to an authorized user of a computer network, computer system; or (4) provides or assists in providing a means of accessing a computer, computer system or computer network; or (5) with the intent to defraud or to abets to false representation, false statement; or (6) to install or tamper others computers, computer system, computer network; or (7) to flow virus or objectionable information e.g., pornography; are cyber-crimes. Knowingly or intentionally both the words represents *mens rea* in cyber-crime and other conducts are *actus reus.*

CLASSIFICATION OF CYBER-CRIMES

Classification of cyber-crime is very complex task because it is new spectacle of crime with ever increasing and ever growing phenomenon but keeping in mind the above discussed elements of crime it can be defined to some extent for the legal purpose. There are several ways of classification of cyber-crime. One way is to classify into main three categories like

(1) Computer is the target as well as victim.

(2) Computer is incidental to other crime.

(3) Crime associated with the prevalence of computers which are also to be called as computer crimes. For example in hacking, cyber theft, cyber blackmailing etc. computer is the target. Sometimes computer is not the essential factor for crime commission but it is a factor to facilitate crime to be speedy and new procedures with quick communications. Here computer is incidental to other crimes e.g., cyber pornography, harassment, unlawful banking transactions and others. Another category is crimes associated with the prevalence of computers e.g. software piracy, counterfeiting etc.

Don Parker identified four forms of computer abuse[6] namely; (1) computer might serve as the victim of crime; (2) computer might constitute the environment within which a crime is committed; (3) computer might provide the means by which a crime is committed; or (4) computer might symbolically be used to intimidate, deceive or defraud victims.

The Federal Bureau of Investigation's National Computer Crime Squad's (NCCS) has given a list of crime categories it investigates. This is as follows: (i) Intrusions of the Public Switches Network or the Telephone Company; (ii) Major computer network intrusions. (iii) Network integrity violation. (iv) Privacy violations. (v) Industrial espionage. (vi) Pirated computer software. (vii) Other crimes where the computer is a major factor in committing the criminal offence.

Another way of classification of computer crime is (1) Offences against the confidentiality integrity and availability of computer data and system which includes illegal access, illegal interception, data interference, system interference, illegal devices etc. (2) Computer related offence e.g. forgery, fraud, sabotage, cyber stalking etc. (3) Content related offence e.g. child pornography, infringements of intellectual property rights etc.We also classify cyber-crime as (1) Unauthorized access, (2) Hacking and fishing, (3) Cracking, (4) Cyber fraud, (5) Cyber theft, (6) Cyber terrorism, (7) Flowing of viruses, Trojan horses, logic bombs etc., (8) Cyber pornography, defamation, (9) Cyber stalking and (10) Spamming.

UNAUTHORISED ACCESS

Knowingly or intentionally use or access without the permission or consent of the owner or possessor whole or any part of a computer, computer system, computer network to commit any cyber-crime as defined above is unauthorized access. This is like criminal trespass committed in the real world. Section 441 of the Indian Penal Code defines criminal trespass as follow:

"411. Criminal trespass. Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property.

Or, having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence,

Is said to commit 'criminal trespass'."

The Computer Fraud and Abuse Act 1984 were revised in 1994 amended in 1996 in the United States to prevent and control cyber-crimes. Spinello (2000) states that these activities: may range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code or command. This Act prohibits unauthorized access to computers to commit other crimes which include access of unauthorized information, access non-public Government computer and others. This Act prohibits unauthorized access to information and protects

confidential information. That whoever knowingly accesses a computer without or in excess of authority to obtain classified information is guilty of unauthorized access even though no damage is caused or value of information is not reduced. Section 65 of the Information Technology Act 2000 in India prohibits tampering with computer source documents and prescribes punishment.

CYBER FRAUD

Fraud committed through computer, computer system, computer network or internet related communications are to be treated as cyber fraud. Any unauthorized access to commit fraud is to be treated as double crime in cyberspace one is unauthorized access which is similar to criminal trespass under s. 441 of the Indian Penal Code and another is commission of fraud after this unauthorized access. According to the National Consumers league, the number of complaints about internet fraud schemes has risen dramatically from 1,152 in the year 1997 to more than 7,500 in the year 1998.[7] Internet fraud can be committed through websites, e-mail, junk mail, spamming, posting a message on an online bulletin board chat room discussion, which is very difficult for the victims to identify whether the act in internet in fraudulent or actual fact.

Section 25 of the Indian Penal Code defines fraudulently that a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise. Section 66, proposed amendment as per the Information Technology (Amendment) Bill 2006, includes the terms fraudulently and dishonestly. The proposed Information Technology (Amendment) Act 2008 prescribed for the application of s. 66 to all contraventions listed in s. 43 by making it as civil wrong for which under s. 43 compensation limit has been removed. And under s. 66 fine increased up to Rs. 5 lakhs. Not only that this section is applicable for dishonest and fraudulent human conducts. The Computer Fraud and Abuse Act 1984, which was revised in the year 1994 and was amended in the year 1996, prohibits using unauthorized access of computers to commit crimes. These are: (1) Espionage, (2) Access unauthorized information, (3) Access of non-public Government computer, (4) Fraud by computer, (5) Damage to computer, (6) Trafficking in passwords and (7) Threats to damage a computer. Illegal use or use or access of computer to cause wrongful loss to others property intentionally or knowingly by any input, alteration, deletion, or suppression of computer database, computer system, computer programme, software etc. are also to be treated as computer related fraud. There are no watertight compartments between several cyber-crimes rather these are very much related to each other. One is sometimes the step or preparation for other and both are crime. For example unauthorized access is a crime which is means to commit cracking or cyber terrorism or other cyber-crimes. In 1984-85, the United Kingdom Audit Commission reported a conspiracy case which is to be treated as input fraud, conspiracy between a local Government wages clerk and about 20 manual employees. The wages clerk made false entries on time sheets. It resulted in the workers receiving additional payments. These processes were shared with the clerk. This process involved a sum of 54,500 and scheme lasted for 3 years. Another example was cited by Audit Commission as output fraud concerning an incident at a computer centre which was responsible for printing cheques. On one Friday evening prior to bank holiday weekend, the staff of that computer centre left the computer suite without authority and in breach of regulations to go to the public. While the centre was closed, no one was there, a theft occurred and a pre-signed cheqe with a value of 9,31,000 was stolen. Subsequently after R. v Gold[8] 1988 case of computer hacking the Computer Misuse Act 1990 was passed. Section 1 of the said Act made obtaining unauthorized access to computer programme or data the basic offence.

CRACKING

Crackers are malicious hackers who usually ‘crack’ down network security. They secretly enter into security system to cause intentional damage. Hackers are most of the times intellectual programmers who have special study and knowledge about computer system and they use their skills to cause trouble, steal credit card numbers, flow viruses etc. of those hackers who are involved in illegal programming act to break into others computer system, and network security they are crackers. So, we can say when hackers cause grievous or dangerous harm to computer and computer system or network security and security system, and break systems, they are called crackers. They not only commit criminal trespass such as unauthorized access but also commit other crimes.

HACKING

Unauthorized use of others computers, computer database, system, network is a crime. Hacking is crime where hackers advance to sabotage, espionage, credit card theft and fraud after gaining unauthorized control of victims’ computers or when they are recruited by serious criminals to advise and assist them. The Computer Misuse Act 1990 and in the U.S.A., the Computer Fraud and Abuse Act 1984 prohibits hacking. Sections 65 and 66 of the Information Technologies Act 2000 in India prohibit hacking and other cyber-crimes. The new Hackers Dictionary, completed by one S. Raymond in the year 1993, defines hackers in number of ways. These are as follows: (i) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. (ii) A person good at programming

quickly. (iii) One who programmes enthusiastically (even obsessively). (iv) One who enjoys the intellectual challenge of overcoming or circumventing limitations. (v) An expert in a particular language or operating system i.e., a UNIX (R) hacker.

However, legal meaning of hacking is associated with the act of obtaining unauthorized access to programme or data held on a computer system or alter, modify or delete etc., any computer programme or attempt to do so, several criminologists have attempted to understand and examine the reasons of hacking or why hackers indulge in delinquent behaviour. Three main theories have been offered: (a) differential association (b) differential reinforcement and (c) social hearing theory. Differential association as described by E. Sutherland is based on the principle which contains numerous conflicting definitions of appropriate behaviors that give rise to various crimes. The person being associated with criminals are to be criminal, they only have to have favorable attitudes towards crime and surroundings.

There are several types of hackers; the word hacker is used to describe all of these: (i) Code Hackers: They knew computers inside out. They can make the computer do nearly anything they want it to. (ii) Crackers: They break into computer systems and security thereon. (iii) Cyberpunks: They are the masters of cryptography. (iv) Phreakers: The combine their in-depth knowledge of the internet and the mass telecommunication. (v) Ethical hackers: Hacker Ankit Fadia and Dr. Neruker in India were identified by NASSCOM and Law Enforcement Agencies as ethical hackers. Thereafter they were working for cyber security and to co-operate with Government to prevent and control cyber-crimes. Hackers are becoming so uncontrollable that it becomes very difficult to cope up with the situation worldwide. Hackers originally were computer professionals who adopted the word hack as a synonym for computer work executed with a certain level of craftsmanship. Thereafter they gradually became desperate for usefulness and accessibility of computer and computer system to citizens. But nowadays hacker and hacking meaning has been changed dramatically. To hack meant to break into or sabotage a computer system and a hacker was the perpetrator of such activities. In early 1960s hacker was an affirmative term because they were intellectual scholars with expert knowledge in Information Technology who could push programmes beyond what they were designed. 1970 was the era of phone hackers called as phreakers such as Captain Church, Homebrew Computer Club through blue boxes, etc. 1980 is remarkable for two hackers group e.g., the Legion of Doom in the USA and Chaos Computer Club in Germany i.e., 2600: the hacker quarterly is the journal to Share tips on phone and computer hacking. Then the Computer Fraud and Abuse Act was passed in the United States which gives more scope to authorities computer emergency response team, which was formed by the U.S. defense agencies with the objectives to investigate the cyber-crimes.

In 1990s hackers break into Griffith Air Force Base, computers at NASA, Koran Atomic Research Institute, Federal websites including the U.S. Department of Justice; Defense Department computers sustained 250,000 attacks by hackers in the year 1995. Yahoo! Was attacked by hackers on Christmas Day 1997 with a threat that unless infamous hacker Kevin Mitnick in released from prison a Logic bomb will go off in Personal Computers of Yahoo's users. In the year 1998, hackers started attack with new shape i.e., spamming and in the year 2004 they started fishing too.

CYBER THEFT

The theft of information or identity e.g., name, date of birth, Social Security Number (SSN), credit card number, password are increasing day by day in cyberspace with other cyber-crimes. In the year 1988, 31st May, in the USA , in support of the Identity Theft and Assumption Deterrence Act, the General Accounting Office (GAO) published a report called 'Identity Fraud : Information on Prevalence, Cost, and Interest Impact is Limited'. The report stated that Social Security Number (SSN) misuse is increased from 305 in 1996 to 1,153 in 1997. Master Card International, Inc. and VISA U.S.A., Inc., stated that losses from their member banks were the $100 million dollars in a year. Master Card stated that 96% member banks loses $407 million dollar for identity fraud in the year 1997 only.Most miserable fact is that victims of identity theft even most of the times do not realize that their identity has been stolen by someone else. Sometimes at the time of further financing e.g., for home, for vehicle etc. they realize from lender that they do not have sufficient credit limit and therefore, they became ineligible for loan for home, vehicle or otherwise. After due enquiry and investigation on credit report those poor fellows may come to know that there is a credit card opened on his name using his identity for which he never applied. Not only that there is a large credit Bill with unknown addresses of creditors. Thereafter, another story will be waiting for them which may be so long that they will get tired; that is, after identifying culprit the proceedings may take months after months or even years after years to end their credit chapter.

Identity theft may be committed due to careless sharing of personal information and identities to intentional and dishonest stealing of digital information from home or public places. Sometimes we carelessly handle credit card and other confidential documents in public place and give information to others about card number, security number, password etc. over phone which may be heard by potential criminals at the time of conversation and they may try to access those documents and commit identity theft. Not only in public places, even at home or private places while we are using our computer or other devices and documents we must do it very carefully so that

others must not access it. The Identity Theft and Assumption Deterrence act was enacted on 30th October 1998 popularly known as Identity Theft Act, was passed to amend existing Fraud and Misuse Act, to enhance penalties in related matters and to make provisions suitable in contemporary social phenomenon to prevent and control Identity Theft or Cyber Theft.

Towards prevention, investigation and prosecution of identity theft seminars, workshops, conferences were held worldwide which proved very helpful to combat identity theft and to enhance law enforcement strategies. Another possible challenge is to communicate victims to obtain basic information for investigation including losses and retreat if any. To achieve these goals law enforcement agencies require interaction with victims and witnesses so that they can make and improve their communication system for any incidents even in grass root level. These communication system and link between Law Enforcement agencies and victims are helpful for victims as well as investigations to access case related information.

FLOWING OF VIRUSES

Flowing programmes through computer network by human agent such as virus, Trojan Horse, Worms, Logic Bombs to cause damage, alter, delete, destroy computer, computer system, computer network, computer database are also cyber-crimes. There are three types of viruses. They are popularly known as file infectors through spreadsheet programmes or games; boot-sector viruses through diskette or hard disk i.e., read into memory and executed when a computer first start; and macro viruses which depend on operating system and infect files which contain data. For example, 'I Love You Bug' virus was the total threat worldwide which was the cause of innovation of several new and more effective antivirus software e.g. Java, Quick Heal, Mobile Antivirus. There are three main characteristics of viruses (1) a virus is a self-replicating programme whose main purpose is to propagate itself at as many different places as possible. (2) A virus can only propagate itself by an unknown act of a user of the system in which it exists. (3) A virus propagates itself by modifying anther programme to include itself.

In R. v Thompson[9] the court held that 'Logic Bomb' is a kind of imputation of a programme into the computer with the intention that when the leading data was entered into the system on that day this input will cause messages which is to be displayed on the screen. Sometimes it may cause more harm and even collapse the system because flowing computer viruses are notorious form of misconduct or misuse which are transmittable from one computer to another computer.

Cyber pornography. Cyber pornography is the growing menace of the day. Section 67 of this Act prohibits cyber pornography. But, Information Technology Act 2000 provides no specific rule to prevent and control child pornography in cyberspace. Now-a-days spamming, multimedia service-video and still pornographic clip and thereby child online pornography are increasing day by day in India like other countries. But only possession is not a crime under S. 67. The Information Technology (Amendment) Bill 2006 and Information Technology (Amendment) Act 2008 proposed to insert s. 67A to prohibit child pornography in cyber space. However, by the Information Technology (Amendment) Act 2008 under S. 67 fine has been increased upto Rs. 5 lakhs and imprisonment reduced to 3 years for 1st instance and for subsequent instance fine Rs. 10 lakhs and imprisonment upto 5 years. And S. 67A prohibits transmission of material containing sexually explicit act and increased imprisonment and fine. Section 67B covered child pornography and prescribed imprisonment upto 5years and fine upto Rs. 5 lakhs for first instance and imprisonment upto 7 years and fine upto Rs. 10 lakhs for subsequent instance. Thus covers grooming and self-abuse through cyberspace. Under s. 67C intermediaries are responsible to preserve and retain certain records for a prescribed period. But this period has not been prescribed in the proposed Act of 2008.

Dr. L. Prakash case[10] on cyber-crime is very significant where the court convicted accused under s. 67 of the Information Technology Act 2000. The accused was arrested by Chennai police for making cyber pornographic image of his clients forcefully.

Mr. Jayesh S. Thakkar v State of Maharashtra[11] petitioner wrote a letter dated 29th May 2001 to the Hon'ble Chief Justice of Bombay High Court about a pornographic site on the internet. And this letter was *suo motu* treated as writ petition. On 28th September 2001, the Division Bench passed order appointing a committee to suggest and recommend ways for prevention and control of cyber-pornography. The committee submitted a report recommending Law reform to regulate cyber cafes and internet service providers.

Cyber terrorism. Cyber terrorism is a kind of cyber threat using new technology or making it target by terrorists. It is national as well as international challenge. Warfare is one way of cyber terrorism by which one nation attacks other nations through Information Way (I-Way). That may be called as Net-War.

International terrorists attack using websites and controlling network i.e., al-Qaida's websites http://www.mojahedoon.net[12] which has link with Osama Bin Laden, attack on Indian Parliament on 13th December 2001 by making false gate pass from internet, 11th September 2001 attack on WTO & Pentagon controlling network of airway, 16th December 2005 e-mail threat to attack Indian Parliament and US consulate are examples of cyber terrorism in India. The Information

Technology (Amendment) Act 2008 introduced Cyber Terrorism as offence by inserting s. 66F and prescribed life imprisonment. Though definition of Cyber Terrorism is not yet clear.

Definition of crime, to find out the causes of crimes proper penal action to reduce crime rate in society are the central objectives of Criminal Science or Criminal Jurisprudence. There are three main branches of criminal science. These are as follows:

(1) **Criminology.** It deals with causes of crime. Whether anatomic structure, social surrounding circumstances or genetic history; which are the contributory factor for crime commission.

(2) **Penology.** It deals with theories of punishment, whether preventive theory, rehabilitative theory, deterrent theory, reformative theory, treatment and correction theory which will be proper in contemporary social scenario to reduce crime rate.

(3) **Criminal law.** This is the substantive law which defines crimes and prescribes punishments e.g., the Indian Penal Code 1860.

Intensive study of several criminologists on cyber-crime have attempted (a) to understand criminal behavior in cyber space (b) to examine the causes for which criminals are involved in delinquent behaviour in cyberspace and (c) to develop effective legal principles for the prevention and control of these dangerous and deviant behaviours. There are three main theories (1) differential association theory as described by Prof. Edwin Sutherland in his Sociological theory; (2) differential reinforcement derived from Edwin Sutherland and Prof. Skinner's theories of learning as contributory factor of criminal behavious; (3) Social learning theory which is associated with the study of Prof. Albert Bandura, i.e., modeling and imitation.[13]

(4) **Differential Association Theory.** This theory is based on the principle that contemporary society contains numerous conflicting structures of norms and behaviours as described by Edwin Sutherland in his book 'Principles of Criminology' in the year 1947.[14] This theory mainly deals with the conflicting definitions of appropriate behaviour which are the contributory factor of several crimes. People through communication with others learn certain behaviour those may be criminal or sober. When they learn criminal behaviour from their intimate groups through communication they generally use the same and in this way commit similar crimes.

In contemporary hi-tech society we find cyber-criminal groups. R. Blackburn in the year 1993 says that peer pressures and peer attitudes influence behaviours of an individual. C. Hollin in the year 1989 accepted the same in his work 'Psychology and Crime: An Introduction to Criminological Psychology'.[15] He says that persons being associated with the criminals have to be criminals have to be criminal and that they only have to have express favourable situation to commit crime.

(5) **Differential Reinforcement Theory.** This theory is derived from Edwin Sutherland's theory of learning as contributory factor for crime commission. According to this theory, criminal behaviour in cyberspace is also learned through the various groups and associations and thereafter this behaviour continues. Therefore, we have to be aware about these groups and their activities to control their actions. Criminals cannot prevent themselves because most of their actions are reinforced and defined previously, i.e. in which manner they will behave are predetermined.

(6) **Social Learning Theory.** This theory is associated with Prof. Albert Bandura's work of imitation. According to this theory, criminals' behaviour are based on learning through observations and actions from other people and application of those in similar favourable situations for which similar result come out that once criminal behaviour is learned, people become motivated to reinforce it. This theory says criminals' behaviours are learned through observation and these are based on observational learning. This learning has three dimensions (1) the family, (2) prevalent subculture, and (3) the social environment. Most of the criminals in cyberspace commit crimes due to passion, addiction to use computer, to act with network, as fun, to take revenge, credit and financial gain.

(7) **Cyber-crime and the Information Technology Act 2000.** In mid-May of 2000 the Indian Parliament has passed the Information Technology Act 2000 which is the Cyber Law to provide for legal regulation of transactions through computer, computer system, computer network. Information Technology Act 2000 has extra territorial application for violation of any provisions of this Act. That if any person violates any provision of this Act from foreign country which affects any computer, computer system, or computer network in India then this Act is applicable in the same way when any one violates the provision of this Act being in India which may result in India and foreign country. For example, IIT Graduate, Kharagpur Mr. Verma was arrested for hacking which was committed from India and with joint collaboration of Federal

Bureau of Investigation of the United States and Indian agency central Bureau of Investigation; of was arrested under Chapter XI of the Information Technology Act from ss. 65 to 78 specially deal with cyber-crimes and penalty.

Sections 65 and 66 are similar in nature. Section 66 prescribes punishment for hacking and other related crimes with computer, computer system and computer network with imprisonment up to 3 years or 2 Lakh rupees fine or with both. However s. 65 deals with tampering a with computer source document for which punishment shall be 3 years imprisonment or 2 Lakh rupees fine or with both.

However, the Information Technology (Amendment) Bill 2006 proposed amendment to Sections 65, 66, 67, 69, 79 and other relevant Sections and inserted certain new Sections in the Information Technology Act 2000. Proposed amended Sections provide for cyber-crimes in general not only for hacking as it was earlier because the term hacking is omitted and words destroy or diminish value of information is shifted to Section 43(i) by the Information Technology (Amendment) Bill 2006. However, the Information Technology (Amendment) Act 2008 proposed to apply Section 66 to all contraventions listed in Section 43 making these civil liabilities and removing compensation limit. Section 66 includes dishonest and fraudulent human conducts and cyber-crimes. Section 66B prohibits receiving stolen computer resources, Section 66C prohibits identity theft, Section 66E prohibits violation of privacy.

Section 68 deals with offence relating to digital signature with punishment. Section 67 prohibits cyber pornography and obscenity in cyberspace and prescribes punishment. Section 69 prohibits activities in cyberspace which goes against sovereignty, integrity, security of India and friendly relations with foreign States and prescribes punishment. This can be called as cyber terrorism. Section 70 prohibits any act in cyberspace which goes against the interest of the Government. Sections 71, 72 and 73 also deal with digital signature. Section 75 deals with extraterritorial application of the Act. Sections 76, 77 and 78 are other preventive and controlling measures.

The Information Technology Act defines Digital Signature in Section 2(1) (p) that it means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the said Act. Chapter II Section 4 provides for authentication of electronic records by affixing digital signature through asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. To verify the electronic records one has to use public key. The private key and public key are unique to the subscriber which constitute a functioning key pair. This digital signature functions mainly in four ways: (1) Confidentiality, (2) Integrity or not tampered, (3) Authentication and (4) Non-repudiation.

Creation and verification of digital signature is encryption and decryption of the private key and the public key for prevention and control of illegal act in cyberspace as well as protection of computer, computer database, information, software, network etc. from any illegal access and attack. The process is as follows: message has been created for the transmission as digital signature by following Hash Function, Message digested and Encryption of private key has been over then it became digital signature and can be transmitted in the form of message. Now for verification have to go to message following Hash Function, Message Digest of one side and Digital signature as transmitted following Decryption public key, Message Digest of that transmitted message. Whether both the message digests are similar or not that is to be verified by the authentic authority, who follow the system, their data, information and other electronic works and devices are more protected then others. This is an effective way to prevent cyber-crime.

Following the Information Technology Act 2000, other Acts, which are amended, are as follows: (i) The Indian Penal Code 1860; (ii) The Indian Evidence Act 1872; (iii) The Reserve Bank of India Act 1934; and (iv) The Bankers Books Evidence Act 1891.

(8) Growing menace of cyber-crime. Cyber-criminals and their new activities with new multimedia technology are going beyond control day by day. It is very difficult to cope up with the situation worldwide without effective, uniform legal framework and preventive and controlling measures. Seldom is there an integrated socio-technical approach to the computer crime problem.

According to Helen Nissenbaum hackers never were part of the mainstream establishment, but their current reputation as villains of cyberspace is a far cry from the early days when, first and foremost, they were seen. Many say that with their deviant behavior, hackers also serve to remind the technological vulnerability and ignorance in our society along with law enforcement officials and legislators. The ever-growing costs for hacking are justified since the hackers have evidently proved that they might be really harmful and if successful, cause even more tiresome and unexpected cost.[16]

Offenders originally were computer professionals and in favorable situation they gradually became desperate and in contemporary social scenario they have started break ins, sabotage, flowing virus, pornographic materials, hacking, cracking, cyber

theft, fraud, terrorism etc. which are playing havoc at times.

Mr. Sailesh Haribhakti, the partner and charter accountants of Haribhakti and company said of a sample of companies which reported cyber-crimes, according to data released by computer security Institute, employee abuse due to internal access privileges accounted for 79 percent, cyber-crimes owing to unauthorized access by insiders was around 71 percent, multiple rating was permitted in this survey. It is the computer forensic and security management which helps to determine who, what, where, when, haw and why doing any act. It also helps to gather enough evidence, investigation, even to detect files but yet are remaining on the system, hidden files, password protected files, encrypted files etc. He again said 'at times, honey pots can also be sued. The idea is to attract the hacker so that his identity can be known. It serves as an early alarm system, but has it downside. When hit, sever all connections with the affected hardware, photo document the system-screen the error message and the log in. Photo document the system showing the configuration in detail, check the RAM and pull the hard disk out and keep in safe keeping. In case of one organization, the proof of the fraud lay in those files which had been sought to be deleted. There is a need to carry out rigorous check, to isolate the time of the event, record what may have happened, prove that something else should not have happened, to enable courts to pronounce a just verdict'.[17]

On 2nd March 1999 news report in almost all newspapers that subscriber of Videsh Sanchar Nigam Ltd. (VSNL) internet service were enjoying a 'pleasant' surprise morning. One subscriber received an e-mail in Mumbai from one Mr. Amitabh Kumar, the Acting Chairman and Managing Director of VSNL, stating VSNLs aggressive price cuts from Rs. 3,500 for a 100 hour account and had slashed rates to Rs. 1,800 for 500 hours account, the rates was down to Rs. 6,500 from Rs. 10,000. There was a voiced e-mail stating VSNL's displeasure over Mahanagar Telephone Nigam Lts's. 'Restrictive Trade Practices' in intentionally blocking some of VSNL's telephone lines. This affects the public sector corporation. That was the first case of system break-in of VSNL. Mr. Kumar said that there was break in and they are trying to trace the person. And he hoped to trace the culprit over the next couple of days, by that time VSNL had managed to trace message of a student's account.

Mr. Pramod Mahajan, the then Union Minister for Information Technology, in seminar on 'Cyber Law and Police' organized by the Central Bureau of Investigation in New Delhi on 23rd July 2000 advised to use hackers and computer experts to check cyber-crimes. New technology is always 'user neutral' and therefore potent in the hands of genuine users as well as criminals. There was need for investigators with 'Crazy ideas' to counter the menace of criminals. If possible take even hacker's help to curb the cyber-crime.

Before amendment of the Indian Penal Code,1860 Dr. R.K. Raghavan the CBI Director said that computer crime had the potential of establishing the country's economy and delivering fatal blows to the banking system. The CBI is gearing itself to cope up with the latest sophisticated trend in criminal activities. At a seminar organized by the Andhra Pradesh State, Dr. C. Rangarajan, Governor stated that most countries had put in place legislation to act as deterrent for computer crime. He suggested for the amendment of the Indian Penal Code, the Criminal Procedure Code, the Indian Evidence Act, and the Copyright Act and to enact law following the Data Protection Act of the UK.

The CBI Director, Dr. R.K. Raghavan said again "the information and communication revolution had converted the world into a small village. At the same time, it posed a serious challenge to the existing and established institutions, practices and law in all the countries. The threat of cyber terrorism was critical because here intelligent criminals were using anonymity as a weapon in cyber space; a legal framework would help control, prevent and detect cyber-crime. He also said that a team of Federal Bureau of Investigation of the USA was here for a week to train our men and this year, two of our officers have gone to the U.S. to acquire expertise.[18] Ankit Fadia at Delhi witnessed a Denial of Service (DOS) attack. He traced its origin within few seconds in Pakistan and alerted the companies and thus a major hack was prevented. He started hacking at 14 years; at 15 he wrote a book on 'ethical hacking' which was punished by Macmillan India. Fadia states that although hacking brings a negative connotation, hackers can be pleasant, intelligent people with the ability to keep cyber-criminals on the run. On 20.01.2005 News line published in Website that in England and Wales's police officers (who have little or no training) are required to receive basic training in tackling cyber-crimes. This training course may be called as 'net crime training and delivery' programme to tackle cyber-crimes because if they don't know what's in front of them how they can seize it! Computer crime is now very much part of main stream policing and any crime have an otherwise Information Technology component.

CONCLUSION

Many laws passed and proposed to grab the criminal activities done because of technology advancement like after Information and Technology Act,2000 the Communication Convergence Bill,2001 in India was drafted to promote, facilitate and develop in an orderly manner the carriage and content of communication including broadcasting, telecommunication and multimedia, for the establishment of an autonomous commission to regulate all forms of communications and for establishment of an Appellate Tribunal and to provide for matters connected therewith or incidental thereto. The Bill also provides in preamble that

whereas it is considered necessary this Act is enacted by the Indian Parliament in the 52nd year of the Republic of India with the aim (i) to facilitate development of national infrastructure for an information based society, and to enable access thereto. (ii) To provide a choice of services to the people with a view to promoting plurality of news, views and information. (iii) To establish a regulatory framework for carriage and content of communication in the scenario of convergence of telecommunications, broadcasting, data-communication, multimedia and other related technologies and services; and (iv) To provide for the powers, procedures and functions of a single regulatory and licensing authority and of the Appellate Tribunal. However, the bill is in cold storage. So, it is suggested to take fast decision to cope up with the speed with which the cyber-crimes are multiplying every moment and it is must in present scenario for peaceful survival as well as in order to grab the cyber-crimes in India.

REFERENCE

1. Lines from the Chapter "COSMOS", in the movie Sneakers, MCA/Universal Pictures, 1992
2. D. Thomas & B.D. Loader: Cyber Crime Law Enforcement, Security and Surveillance in the Information Age, London & N.Y Routledge, 2000, p. 3.
3. Ibid.
4. S.T. Viswanathan (2001). The Indian Cyber Laws: with Cyber Glossary, (BLH) New Delhi, p. 81
5. See generally J.C. Smith and B. Hogan (1988). Criminal Law, 6th Ed., Butterworth and Company Pub. Ltd. London.
6. Donn Parker (1993). Crime by Computer, (NY : Seribner) 1976 cited in 'Computer Law' 2nd Ed., by Chris Reed, p. 203.
7. Press Release: "NCL Release Top Ten Internet Scams" at http://www.natlconsumers-league.org/top10net.htm.
8. [1988]1 AC 1060; see also [1987]3 WLR 803.
9. [1984]3 All ER 565.
10. For detail see http://www.naavi.org, www.ciol.com/cybercrimes/news etc.
11. For detail see http://www.cyberlaw.org/cybercrimes, www.opera.com.
12. Internet and American Life Project, 5th September 2001; for detail see http://www.pewinternet.org/news/"NUKEOSAMA+SADDAM+CASTRO NOW!!!...+ BUYGUNS+…
13. Gattiker, U. & Kelley, H., 1997 Technorime and terror against Tomorrow & # 8217; organization: what about cyber parks http://hostnome.ncsa.com Directory: Library.
14. Edwin Sutherland: "Principles of Criminology", 1947, 4th Ed., pp. 82-85 Philadelphia: Lippin cot.
15. New Yeork (NY) Rout ledge.
16. D. Thomas and B.D. Loader: Cyber Crime Law Enforcemtn, Security and Surveillance in the Information Age, 2000, p. 56.
17. Insiders account for 79% of cyber-crimes, on 14th June, 2000, Economic Times published.
18. S.T. Viswanathan: The Indian Cyber Laws with Glossary, BLH, ND, 2001, India, pp. 88-91.

Corresponding Author

Rawat Singh*

Research Scholar, Department of Law, Maharaj Vinayak Global University, Jaipur