THE CONCEPT OF CYBER-CRIME: NATURE & SCOPE

VIJAYKUMAR SHRIKRUSHNA CHOWBE
Associate Professor and Head, Post Graduate Teaching Department of Law, Sant Gadge Baba Amravati University, Amravati, India
vijuchowbe@gmail.com

ABSTRACT

Cyber crime is whether myth or reality? Nothing is crime unless prescribe by law. But most of the categories of cyber crime is still beyond the reach of law. Even there is lack of unanimous consensus over the commonly agreed definition of 'cyber crime.

Present article has attempted to conceptualize the 'cyber crime'. The analysis is from legal point of view and various aspects are touched upon. A cursory glace has been given to whether cyber crime can be accommodated within the existing legal framework or does it require a complete new approach? This article has analyzed the operational modality to combat cyber crime and its probable difficulties in the traditional system which is based on different principles, which in cyberspace hardly respect and difficult to govern. The objective of these analyses is to verify the compatibility of legal system to coupe up with such techno-sophisticated criminality.

KEYWORD

e-technology
cyber crime
cyberspace
Computer

PREAMBLE

The advent of e-technology has brought variety of opportunities and some of these, not surprisingly, are of a criminal nature. The Cyberspace created by computer technology provides a medium of doing many things in efficient manner. The use of machine replacing human hands provided greater opportunities and options. The automation of companies, banks, educational institution, and railway reservation are reflections displayed everywhere that manifest dependence of human society on these tiny computers. Today, old-fashioned paper-based working pattern is merely outdated, as it is unable to keep pace with speedy life of modern world.

Societies world over in the last century have been largely concerning about crime affecting the physical persons and property. They have accordingly evolved state systems of law and enforcement to deal with the forms of crimes. Rapid industrialization and urbanization has brought new forms of crimes involving wider concerns of social order, safety, and security.[i]

If Cyberspace is the type of community - a giant neighbourhood made up of networked computer users around the world - then it is natural that many elements of a traditional society can be seen as bitts and bytes.[ii] With electronic commerce, emerge electronic merchants, plugged in educators provide networked education and doctors meet with patients online. It should come as no surprise that there are also Cyber criminals committing Cyber crimes.

Computer-technology helps any company to do work efficiently. The computer is a very sophisticated electronic machine used to manipulate data. As explained in the glossary of the Information Technology (Certifying Authorities) Rules, 2000,

'Computer mean any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network'.[iii]

Motivational factors for the growth of Computer Technology

The information, which is a very important aspect of every business and transactions, can be move very easily and manipulated in better manner with computer-technology. The Computer-machines are now-days overtaking the responsibility assigned to human brains. In addition, in this attempt it is providing better alternatives. A brief comparison of computer technology can be displayed in following manner:

a. **Computer has great memory power**. It provided huge storable space on comparatively very small floppy's and CDs. The entire library can be put in few computer discs.

b. **The speed of manipulation** of available data is **unimaginable**. The Computer can solve complex mathematical problems in seconds. The loan interest, for example, of the person standing in front of bank counter can be calculated in a fraction of seconds with accuracy.

c. **Computer can work round the clock.** Computers never form unions, ready to work anytime. Thus today, ATM machine facilitate the banking transactions 24 hours, which earlier were just restricted to few hours a days.

d. **Computer can do multiple jobs at a time.** Thus the same computer can ask to calculate pending matter, subtract a specific data, can be asked to present a show at specific time, able to maintain time schedule, and even can be asked to distribute the massage to thousands of customer.

e. It is old saying that '**No man is perfect on this earth**'. However, it is possible with computers. Computer only commits mistake if programme fed in it is wrong. There is a little bit of chances of committing mistake by computer itself.

All these plus points are responsible to replace man with machine and there is continuous dependency of human society on the machine. Ultimately, under the background of this machine power, the maximum institutions started to equip themselves with machine; the process is generally known as '**AUTOMATION**'.

The process of automation can be considered with the process of '**URBANISATION**'. When industrial revolution took place in the Mid-Seventeenth century, the big machines appeared on the scene. The industrial plants, turbines, ships started to appear and soon rural population started to migrate towards big cities. After a couple of century, we could see that the urban society is entirely different from rural one.

Thus, the wave of industrial revolution caused urbanization of rural society and completely transformed it. Urban society is different from rural one having slum areas, big industrial plants, cotton mills, working industrial population, poverty, fast life and so many things are the symbolic features of urban society. The weak tie of human relationship, degrading human values, flat & apartment culture, fashions, clubs, spacious roads, flyovers, railway bridges, dance bars, easy flow of money, 24 hours working, crowdie places, departmental stores, big moving vehicles waiting at signals, commotion of railway engines and begging children are some of the common scenes in urban society which are hardly visible rural society. As life, so as to crime differ in urban society. As money is move valuable than values in urban society, economic crime rate is more. Due to lack of fraternity, neighborhood belongingness in urban society, criminal even can commit dacoit in daytime. Minimum social pressure, lack of social control makes urban society very different from rural one.

As the 'Urbanization', so as the 'Cyberisation'. The same change that we have seen in the process of urbanization can be similarly observed in **Cyberisation**. While human being is Cyberised (or treat it as de-socialized), they are losing and lacking human qualities, no value and respect for relations and relatives. In Cyber world, you can find youths spending their time in chatting, looking sex partners, surfing for pornographic material. Cyberisation, in other way can be termed as revolution of Information-Technology. This Information-Technology revolution is enormous than earlier revolution has taken place so far, and the changes and transformations it has caused in the society is also comparatively immense. In Industrial revolution that took place a couple of centuries ago highlighted the presence of big machines likes steam engine, locomotives, ships, cranes were appeared, but today, tiny machine are there sometime only with three components i.e. Monitor, CPU and keyboard which can be kept in small space of 5 fts X 5 fts room. However, potential capacity to change the society is much greater than else before. This device as compare to olden day's ship can travel its user faster and can escort the netizens in any part of world, can make possible his virtual presence.

Thus these connected computer machines has created a different world called Cyber-world or Cyber-space. It is a different world altogether. Quite different from our real world! Due to special nature of this Cyber-space, the Cyber criminals get maximum opportunity to commit crime. Because computer may facilitate the commission of traditional nature of crime like fraud, theft, defamation, pornography in new form as well as give rise to new mischief's such as hacking, virus transplantation, erasure of programs or data.

Under this backdrop, it is essential to analyze and understand the different nature of Cyber-crimes, its definition, scope with comparative analysis with that of 'old-traditional' criminality.

COMPARATIVE INVESTIGATION OF CYBER-CRIMINALITY AND ITS NATURE

I. **Comparative analysis: Modern & Traditional crimes**
II. **Incidences of Traditional crime - easy to deal**

To understand the sea change computer technology has introduced to criminal activity, the hypothetical example may dictate it properly: Consider this one,

> 'One can analogize a denial of service attack to using the telephone to shut down a pizza delivery business by calling the business telephone number repeatedly, persistently and without remorse, thereby preventing any other callers from getting through to place their orders. While it may be possible for someone to execute this scheme, it would be very onerous to do so because it would require a great deal of physical effort and concentration on the perpetrator's part; he would have to be constantly dialing, maintaining the connection until it was broken and then redialing quickly to prevent any other call from coming in. It would also involve a significant risk of apprehension because the victim could contact the authorities, who would presumably have no difficult tracing the calls to the perpetrator, since he would presumably be using his personal or business telephone.[iv]

The incidence of traditional crime, most of the time, is easy to deal by law regulating agency. Here location can be traced out, person can be identified, facts and issues can be investigated, telephone calls can be scrutinized, `***mens rea***' can be ascertained and liability can be imposed. However, in the incidence cited above, the legal machineries may be paralyzed to deal with above-mentioned problems. Generally, and in most of the traditional crime cases, the problem of jurisdiction may not arise in above case, physical search is possible and above all, the law applicable to both perpetrator and victim is same. Too great extent, the traditional legal system is well equipped to handle, investigate, scrutinize, and examine the facts related to the crimes.

Demarcation between Cyber-crime and that of so called traditional crime can be traced out on some distinguished footings. However, ironically, one may mislead term in physical sense. Thus physical harm inflicted to computer, stealing of computer machine, theft of computers from the home or institute or any part of computer such as hard disc, monitor or keyboard, making fraud in selling computer machine is not computer crime though on first sight it may seems to be 'Crime committed against a computers or by means of computer' OR 'Harmful act committed from or against a computers or networking. The description of Cyber crimes given above as elaborative sense.

Cyber crime is easy to commit (if one has the know - how to do it), hard to detect (if one knows how to erase one's tracks) and often hard to locate in jurisdictional terms, given the geographical indeterminacy of the net.[v] The ability of Cyber criminals to morph into new and different forms of antisocial activities evading the reach of existing penal law creates challenges for law enforcement around the world. Cyber-criminals can exploit gaps in their own country's criminal law to victimize their fellow citizens with impunity. They can also exploit gaps in the criminal laws of other countries to victimize the citizens of those and other nations.[vi]

INCIDENCES OF CYBER CRIMINALITY

Relatively, in case of Cyber-criminality, Cyber space allows these attacks easily carry out and such intrusions can be made effortlessly with very little risk of apprehension. First of all, it is very difficult to fix the identity to the perpetrator in Cyber-space as it is very easy to mask a fake identity. You can have a mask of famous hero, heroin, politician or even policeman with photo-identify in the Cyber-space. It is difficulty to see the person actually sitting in front of terminals and only the manifested identity is only source in Cyberspace. Secondly, it is difficult to locate the jurisdiction and locality of the perpetrator. Neither it possible his intentions and benefit he receive from such deviation. However, one can face these preliminary difficulties in Cyber-space.

i. Cyber-crime is not synonyms with Internet crime

Generally, it is mistaken belief that Cyber-space is synonyms of crime committed across the Internet-networking, as former is much wider expression encompassing - besides Internet, the computer and its networking, data present in digital form in the computer or on any storable devise, software and hardware in any functional form. Cyber crime may be committed even by remaining offline and it is not necessary that the person should physically remain present online in the networking of computers. Thus software piracy is the crime committed by the person by taking the software copy on disc or floppy and transmits it.

ii. The fashion of 'Computer literacy' fasten the process of Cyberisation

Today the courses pertaining to ‘computer literacy’ training become an integral part of curriculum. Due to the vast use of electronic devices within the atmosphere available around the new generation, the new generation very easily got electronic indoctrination. Right from the age of spoon-feeding, electronic technology surrounds them. Thus, when they come out of their tender age and got capability of stepping into Cyber-space, vast Cyber-world open a getaway for endless opportunity. However, due to tender age and lack of judgment capability there are equal chances of their exposure to the evil effect of this technology. Thus on one hand, technology that is an essential part of their curriculum hurled them in the unprotected Cyber-world.

iii. Cyber Crime - Neither difficult to learn nor difficult to commit

Cyber-crime is neither much hard to learn nor much difficult to commit. In modern society, computer technology can be learned like language. Digital technology surrounded our life to such a great extend that everybody is being acquainted with it. Particularly, the new generation for whom computer knowledge is an essential part of curriculum, and where knowledge diffusion is with the help of computer it is very easy for them to have convenience accessible means to commit crime in Cyber-space. Incidences are there, where initially, computer is learned either out of curiosity, pleasure or compulsion (may be official or educational) or latter on learning knowledge turned into delinquency. The user-friendly software has added fuel to the fire making Cyber delinquency much pleasant and easy. This is true, particularly with regard to pornography, vulgar chatting, and piracy. Today, anybody with minimum computer literacy is sufficient to have access to Cyber-criminality and the chances are very less of being trapped by the preventive agencies. These features make Cyber-crimes more dangerous and alarming.

iv. Difficulties in tracing the Cyber crime

If one is enough fortunate to overcome these difficulties of locating, investigating and fixing the criminal liability, the next complexities he has to face about the collection, examination, scrutiny, instigation and recording and reading the evidences and witnesses. Speaking with example, suppose in the example of Cyber-stalking cited above, perpetrator used computer for the purpose of hacking and stalking the web site of pizza parlour via Internet, how can the recording and reading of evidence is possible even if, the instrumentality of an offence i.e. computer has been seized? Again, whether does legal system has capable of recognized such evidence in electronic form? Suppose, again the hacking or stalking has been committed from paid Cyber-café, then how the presence of criminal can be located? In short, such problems make Cyber-criminality more severe and serious in this millennium.

In addition to that, as due to Internet facilities, Cyberspace don't recognized boundaries, barriers or line of control of the nations, the problem of jurisdiction also create problem in Cyber-criminality. Thus the potentiality of Cyber criminals to morph into new and different forms of antisocial activity evading the reach of existing penal law create challenges for law enforcement around the world. Cyber criminals can exploit gaps in their national criminal law to victimize their fellow citizens with impunity. They can also exploit gaps in the criminal laws of other countries to victimize the citizens of those and other nations.[vii]

v. Are there any alternatives to Cyber technology to avoid Cyber criminality?

The situation mentioned above creates a dilemma. Should we reject the technology at all to avoid its evil effect on existing system? Should we take a pause for progress as it does bring uncertainty and complexities? Should we stop at the point where we are and just try to maintain present system as it is? Should we stop the use of Cyber-technology to stop its misuse and its dangerous impact in the form of Cyber-crime?

Do at all such objective alternatives are possible for us? Can we stop the flow of time and change? Can we bring to a halt (and lock up) all inventions and discoveries oozing out of laboratories? If this is not at all possible to reject invented discoveries, what are the other alternatives available for us? In this situation, whether is it possible to taste the fruits bypassing or avoiding its drawback?

No doubt, that there are growing incidences of misuse of Cyber-technology, particularly Internet services that include all Cyber crimes and the Indian scene is not exception to Cyber-criminality. Today, the cases are comparatively less than advance countries (despite the Cyber-illiteracy in India, most of the cases neither detected, reported, not bring into light or gone unnoticed, or fall victims of our traditional legal infrastructure) the pace with which the automation process is going on in India, the days are not far when we require to either reject the technology or safeguards against its probable threat. It is even unwise to reject the technology because crimes are committed online. The online crime commission rate is not strong reasons rejecting the entire technology particularly when its use outweighs its misuse. It is just like telling the people to avoid use of vehicles, as there are chances of accidence, or telling the people not to come out of their homes, as there is danger of life in outside world. On developmental path, no U-turn is allowed and once you step in the process, there is no way out.

Do you think that people would avoid using Internet due to growing number if net abuse? Specially, when visionary eyes can see the bright future through Cyber-technology, particularly education, business, banking, and information sharing services are switching over through the network. Under these considerations, should anyone dare to say, 'Avoid/Reject getting misused'. In short, Cyber technology is non-optional, and we have to have it!!!

vi. If Cyber technology is non-optional, there is only one way - accept it boldly

Such questions lead to give a thought for development of system for prevention and control of Cyber-crimes. Whatever the impact of automation on human civilization may be, but it is non-optional phenomenon in competitive life and we have to accept the presence of electronic devices in every walk of life. These electronic devices are so deeply penetrated in our day-to-day activities that we even cannot imagine life without it! All activities in our life such as trade, business, transaction, communication, transportation, invention, education, calculation, medicine, and banking involve use of computers. Thus, today **'*Life without computers*'** can't be imagined.

Today information is a life-blood and important for our existence. Life minus information will reduce the human society to just its physical existence. Information makes man think and act and thus become pre-requisite condition of human expression. Information is one of the indexes of demarcating a line of distinction between human and animal. Information in electronic age is synonyms with either power or source of power. In order to survive in competitive market, information is essential. It is only due to advent of electronic era, information got electric speed and it is possible to remain up-to-date (may be up-to-fraction of second) with the help of electronic devices. In the absence of this system, the market would never survive for the next moment.[viii] Today, computer networking is providing electric speed to the information and magnetic brain to store information and manipulate with the help of software. Nevertheless, this field is also not exception to the Cyber-criminality. The piracy, theft of Internet hours, Cyber-bombing, e-mail bomb, and Cyber-terrorism are certain brand names from which alarming signals are blowing.

vii. Strategy to be adopted

The problem of Cyberspace starts with the non-recognition on the part of legal system. Generally, and at most of the occasions, it has been observed that legal reality differ from bookish philosophical notions appears in law books. Cyber law exists at the (cutting) edge of law, where the ability of existing law to achieve its goals is challenged. In this sense the "law" in Cyber law is a much broader concept, it is "law in action" as opposed to "law in books" as it applies to situations where Law cannot cope. Moreover, the technological revolution has wrought in its wake various security issues and there was an urgent need for security experts as well.[ix]

But so far as strategical aspect in Cyberspace is concerned, it is now a need of an hour to face it, rather than ignoring or running away from it. It is wise saying that ***'don't avoid, face it'*** and it is equally applicable to Cyber-technology also. Positive attitude and clever move demands the adoption of intelligent strategy. Proper use is better than no-use. Thus regardless of thinking about avoiding technology, we can work out a plan for its proper use. Instruction, awareness, consciousness, and Cyber-literacy can be the golden rule for using Cyber-technology. Speaking on the same line, one of the famous website promoted the awareness amongst the netizens.

A better strategy would be to instruct netizens (children) about both the benefits and dangers of Cyberspace and for them to learn how to be "net -wise" in order to better safeguard themselves in any potentially dangerous situation. Make sure the kids know it is okay to approach you if they receive strange or harassing e-mails that makes them uncomfortable or they accidentally get to a site you have told them is not appropriate. Let them know that you won't get angry and that it isn't their fault if they do get something strange or they find a site by accident. Establish the ground rules and let the kids clearly know what they are. Every family is different and every child is an individual, so there are no 'magic rules' to follow beyond the basics. The more open you are and the more you listen, the more likely they are to tell you what is going on. Most of all set a good example by yourself visiting good site![x]

viii. Cyber criminality naïve the traditional boundaries of nation wide jurisdiction

The Cyber criminality, as stated earlier, spread in the Cyber-space and the Cyber-world is too great extent differ in quality and its quantum with that of traditional world. These qualities are: its lack of respect for jurisdictional boundaries, the sheer volume of traffic that it can handle virtually instantaneously, its openness to participation, the potential for anonymity of members of the virtual community, its apparent economic efficiency. It is these very qualities of Cyberspace, which has today become its nemesis and has necessitated the need for Cyber law.[xi]

Thus these are the various angle of Cyber-criminality and related issues. Attempting to scrutiny whether the Cyber-crimes are reality cause any threat to India, the nation where it is in just infant stage? Whether Cyber-crime has become reality in India, or it is just an '***Abominal story***'?

CYBER CRIME ON INDIAN SCENES

i. Cyber criminality - dawning reality in India

Evidently, he was William Gibson, American Novelist by profession, who introduced the word 'Cyberspace' in his famous novel *Necromancer* in 1984.[xii] It has subsequently become widely used as a means of denoting the apparent or virtual location, within which electronic activities are undertaken.[xiii] By 'Cyberspace' in the novel **'*Necromancer*'**, he was insinuated the visual world breathing in electronic activities. The fictitious world was capable of pretending visual reality, totally mechanical and electronic! The 'Cyberspace', according to William Gibson, where the visual reality exists, and the overall populous are immersed & emerge in the digital world. Thus, the aggregation of computers, Internet, and intranet is dubbed as Cyberspace. Such a Cyber networking allows citizens of a community to connect to the global computer communication network and provide them with the facility to communicate with other members of their own community and with the world, popularly, branded as netizens. Therefore, the netizens are net citizens, who utilize the net from their home, workplace, school, library, etc.[xiv]

And today, the Cyber crime has become reality in India. Difficult to detect, seldom reported and even more difficult to prove, computer-related crime lacks a traditional paper audit trail, is away from conventional policing and requires specialists with a sound understanding of computer technology.[xv]

ii. Modern Technology has activated mechanical transformation of human being

The modern technological inventions have brought with them some evils that now creating alarming situation that required urgent attention. In the modern age of communication and electronic transactions, the compelling need of automation to be remained in competition, dependence on mechanical speed created a bridge between man and machine, life and non-life entity, natural brain and artificial brain. These two extreme poles, man and machine, representing life and non-life entity is losing their unique qualities and moving towards each other. In the present scenario, erosion of human qualities and dripping out of human being, and advancements are made to add more human qualities to adroit i.e. artificial robots. In post-modern era, each object is losing human sensitivity evaporating its conceptualized base with its referenced boundaries, emotions, happiness, sorrow, love, affections, responsibility, values and much more 'life' itself. New technologies today provided sky-less limit and speed breaking the boundaries.

CONCEPTUALIZING CYBER CRIME - DEFINITION, ANALYSIS AND EXPLANATION

iii. Legal literature only prescribe, not describe Cyber crime

The law only prescribes the things but do not describe it.[xvi] Particularly, penal laws prescribe the punishment but do not attempt to describe the crime and its nature. Therefore, the legal literature hardly helps in this regards. It is unwise, therefore, to describe here Cyber Crimes, as ***"acts that are punishable by the Information Technology Act, 2000."*** Because the Information Technology Act, 2000 neither define nor describe any of the Cyber Crime. It has only stipulated certain act as an offence and prescribed punishment under Chapter XI titling "Offences".[xvii] However, various jurists, thinkers have attempted to define the term Cyber crime from various angles. Here in this portion we are going to consider some of the definition of Cyber crime in order to elaborate and understand term.

iv. Conceptualizing Cyber Crime - Mapping different dimensions

To deal, it is essential to limit the concept within the word's boundaries. It is helpful to encompass it within a literal periphery. Elaborating any concept from definitional point view is an attempt to attach some meaning full words for its explanation. Defining the concept is nothing but to endeavoring *'Why the things are things and not otherwise'*. In other words, by definition of Cyber crime, we are trying to explain why Cyber crime is Cyber crime and not otherwise. The overall definitional part deals with the aspect of separating Cyber crime from other crimes and clarifies from other so-call similar words. Thus, it is an activity of putting similar things together and isolating it from dissimilar things.

v. Definition of Cyber crime - encircling the concept within words boundaries

In order to understand the Cyber crime at conceptual level, it is essential to scrutinize the definitional aspects of word ‘Cyber crime’. In this portion, some of the definitions are verified.

i. **According to the website of Crime Investigation Department, Andhra Pradesh State Police, "Cyber crime means Unlawful acts wherein the computer is either a tool or a target or both."**[xviii]

According to the definition, the Cyber crime consist crimes-

a. **Where the computer is a tool for an unlawful act - and;**

b. **Where the computer is the target for an unlawful act.**

c. **Where computer is both tool and target for/of unlawful act.**

Ii. According to Manish Lunker, -

> ***"Computer or Cyber armies are considered as illegal, unethical, or unauthorized behaviour of people relating to the automatic processing and transmission of data, use of Computer systems and Networks".***[xix]

However, the present definition considers Cyber-crime and computer crime as one of the same thing, which though having some common premises, differ on several account. Again, this definition have rider like 'unethical' which, too great extent, fall outside the purview of law. Ethics is not basis for imposing legal liability.

ii. Another definition of Cyber crime may be considered as follows :-

> **"Cyber crimes are the harmful acts committed in Cyber space *with, on or by means* of computer networking."**

iii. The a further definition has given by Pavan Duggal, an advocate of Supreme Court and Cyber law expert, “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of Cyber crime".[xx]

Thus in Cyber crimes ‘computer’ may be –

a. an instrument and/or
b. target and/or
c. Means for commission of crimes.

iv. According to Balwinder Singh, Additional Secretary, Central Vigilance Commission, Government of India[xxi], "Computer (Cyber) crime mainly consist of unauthorized access to computer system, data alternation, data destruction, theft of intellectual property."[xxii]

> **“Any crime with the help of computer and telecommunication technology”, with the purpose of influencing the functioning of computer or the computer systems.**[xxiii]

There are some more definitions appear in the literature

1) Cyber-crimes can also be described as "Crimes committed against a computers or by means of computers’ OR ‘Harmful act committed from or against a computers or networking.'[xxiv]
2) Cyber crime is commonly referred to as a "Criminal activity related to technology and computers committed on the Internet."[xxv]
3) According to MyCert’s manager Solahuddin Shamsuddin, "Cyber crimes includes illegal activities done with malicious purposes from electronic hacking to denial of service attacks that cause great loss in monetary terms to the affected victim."[xxvi]
4) According to Charles Nesson &, Anita Ramasastry, "Cyber Crime" is embrace criminal acts that can be accomplished while sitting at the computer keyboard. Such acts include gaining unauthorized access to computer files,

disrupting the operation of remote computers with viruses, worms, logic bombs, Trojan horses and denial of service attacks; distributing and creating child pornography via the Internet, stealing another's identity; selling contraband and stalking victims."[xxvii]

vi. Analysis of Definition - How so far Cyber Crime can be suitably described?

Above definitions have been attempted to describe Cyber Crime from one or the other angle. Depends upon the approaches it adopted, the above definitions can be classified as descriptive, functional, elaborative, purposeful or expressive. The above-mentioned definitions have been attempted to define Cyber Crime by affixing some rider, characteristics, and qualities to the nature of Cyber Crime. Some of the characteristics features of Cyber Crime can be categorizes as -

a. Cyber Crimes are Unlawful Act.

b. Computer is essentially an element of Cyber Criminality and it is either a tool or target of Cyber Crimes.

c. Cyber Crimes are harmful Act.

d. Cyber Crimes are committed in Cyber-space with the help of Computer networking.

e. Cyber Crime is a criminal activity where Computer can be used to perpetuate further crime.

f. Cyber Crimes are committed against computer or computer networking either by means of computer or otherwise.

g. Cyber Crimes are committed from or against computer networking.

h. Cyber Crimes are criminal activities against technology and computer committed on Internet.

i. Cyber Crimes are illegal activities done with malicious purposes.

j. Cyber Crimes cause great loss in monetary terms to the affected victim.

It is, therefore, clear from above discussion that Cyber Crimes are a sort of hi-tech criminality and harmful activities occur in Cyber space created by interlinking of computer networking via Internet.

CRITICAL APPRECIATION OF DEFINITION OF CYBER CRIME

Definitions appear in above section given by various jurist and thinkers have been attempted from various angle. To great extent, not a single definition attempted above compressively describe the Cyber-crime and it only attempted to describe the Cyber crime from the approaches adopted by the jurist and thinkers. Broadly, the above definitions can be categories into four part based on the approach adopted;

a. From its effect on a general society, it (Cyber crime) is :

i. Unlawful act,

ii. Harmful act,

iii. Illegal activities

iv. Criminal activity

b. From victim's point of view -

i. Affect victim and

ii. cause great loss in monetary terms

c. Considering essential tools used in Cyber crimes - it means when following things are utilized in committing crime -

i. Computer

ii. Technology (IT)

iii. **Computer networking**

iv. **Internet**

d. Considering the place where Cyber crime committed,

i. **In Cyber-space.**

EXPLORING THE DEFINITIONAL DENOMINATIONS

The various definitional denominations affix to Cyber-crime by various jurists, thinkers, and legal luminaries cannot be put beyond criticism. None of the definition of Cyber-crime, if scrutinized from jurisprudential aspects, can pass the test on legal standard. Because, the words used in the definition like, 'unlawful', 'illegal', 'harmful', 'criminal activity', 'monitory loss', et al., is difficult to encompass within the jurisprudential limit and sometime, either Cyber-crime or the literary limit of these words cross boundaries and step out of legal premises and require to study the concept from social, political, economical or even psychological point of view. This is equally true with other phenomenon.

For the time being, therefore, the careful analysis of these definitions from jurisprudential angle revealed certain cynicism.

Firstly, it is erroneous to brand Cyber crime as **'unlawful'** act. For any act to be unlawful, the prior existence of legal prescription declaring a particular act is necessary. No doubt, that Information Technology Act, 2000[xxviii] deals[xxix] with some of the Cyber crimes, but all the catefories of Cyber crime have not been covered by the act,[xxx] and therefore, some of the Cyber crime still falls out of the legal reservoir. In short, the test of 'unlawfulness' makes only some of the Cyber-crime within the preview and keeps most of it outside. The same criticism can be made about those definitions describing Cyber crime as 'illegal' or 'criminal' act.

Secondly, it is wrong to say that Cyber crime is **'harmful'** act, though most of the Cyber crime may be, but there are some of the categories of Cyber-crime, which are not strictly, consider as harmful. For example, viruses are not harmful, unless and until they are activated. There are some of the viruses, which lay within the hard disc and activated only after clicking a particular program. Therefore, unless a specific program is not comes into operation, these viruses lie as usual and do not sustain harm. Another example can be given of those persons who use fake identity but while surfing they cast votes, give their opinion, take part in good discussion, or even make some academic conferences while chatting. In such situation, the person whose identity has been used, sometime benefited by such act. The incidence can be compare with the famous case of **Ashby V. White** where the person whose legal rights were violated did not suffer any harm, loss or damage in monetory sense. Thus, harm, loss, or damage cannot be considered as the only criterion for describing any act illegal. Actually, it is misuse, not harm, which is basic ingredient here to be considered.

Thirdly, again, the terms like 'against computer', 'on computer' seems to be misleading. These definitions make all those acts as a Cyber crime, which is committed on, by or against the computer. Thus, it will include the act like theft of keyboard, mouse pad, hitting a computer by stick, or even making electric power off while computer is in operation, which causes loss of data! Logically, all these acts are committed on either by or against the computer, but cannot consider as categories of Cyber-crimes.

Fourthly, the terminologies like 'Cyberspace', 'computer networking', 'technology', or 'Internet' needs further clarification and in absence of such clarity, any definition that includes such words make situation more vague and worse than before.

The definition, at this point, that seem more accurately describing Cyber crimes is -

"CYBER CRIME IS HARMFUL ACT OR MISUSING COMPUTER TECHNOLOGY."

The above definition to some extent expresses Cyber crimes, though the word ‘misuse’ again creates some difficulty. In what sense should the word ‘misuse’ be interpreted? Tentatively, the misuse here has been considered setting international standard within the focus. As stated earlier, Cyber-crime is trans-national criminality and therefore, attempting its definition totally from the point of view of private international law may create some difficulties.

vii. Cyber Crime and related terminology

In order to understand Cyber crime, from the point of view of definition mentioned above, it is essential to give a thought to the words like Computer networking and Internet. Computer networks are telecommunication highways over which information travels. Section 2 (j) of the Information Technology Act, 2000 defines computer network as:

The interconnection of one or more computers through the use of satellite, microwave, terrestrial lines or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.[xxxi]

In simple words, a computer network is purely a system of interconnected computers. Secondly, the word Internet is world wide interconnected networking of computers. The difference between computer networking and Internet is that of degree. Because, Internet is a wider concept where the computer is linked to rest of the world via networking which is available and spread over the world. However, computer networking may spread over to the world, to an organization, to a single premise, or even restricted to the single room. The depending upon the area it cover, computer networking may be classified as WAN (Wide Area Network) and LAN (Local Area Network).

SCOPE OF CYBER CRIME

The next issue under discussion is ***whether really Cyber crime are worth important to be considered on different footing than traditional criminality****?* The answer is simply **' YES'**. Justification, however, can be argued under following heads;

viii. Does Cyber Crimes are worth to take seriously?

Until a couple of year before, 'crime' was small-scale, simple, and consistent and can be traceable with available tools. It is simple in the sense that nationwide generalization, wide definition capable of encompassing within the words limit is possible. Even declaring any act as an unlawful by legislative enactment prescribing punishment for its violation was enough to lower down crime rate. Most of crime and related phenomenon remain personal, and though wide, it remained small-scale. Thus until recently crime is treated as anti-legal and anti-social activities committed by illiterates, (except While Collar Crimes & Organized Crimes), impatient, mentally weak person, or committed under sudden provocation, under tense emotional stress, or sometime out of necessity, or exceptionally, to settle the score with victims.

Again, these simple types of crime are easily traceable with available tools. As most of the crime are of personal nature, and both accuse and victim share same community tie that put offenses into a manageable, knowable context. In short, criminality as we traditionally have understood, wrapped by social atmosphere where social pressure use to keep criminality within manageable limit, either exerting social knots or socially oriented approved system. The social atmosphere not only mount a sort of buffer solutions, but also gave citizens at least the illusion of security, the conceit that they could avoid being victimized if they avoided certain activities or certain associations.

ix. Cyber Crime - Where the difference lies?

Difference between Cyber-crime and traditional crime

First of all, Cyber crime is essentially committed on or with the help of Cyber technology. Therefore, nature and scope of Cyber-crime should be analyzed on different footing. Therefore, uses of computer, an electronic device, for the commission of crime is essential ingredient of Cyber crime. However, traditional crime does not have such condition precedent.

Cyber-crime differ from so-called traditional crime because Cyber-technology provides wrongdoer special conditions where he can hide his identity, even wrongdoer can use fake identity, he can have access the computers of victims without his knowledge and without any restrictions. Here no national boundaries can restrict the entry of wrongdoer. At the same time, procedures developed to trace out the traditional crimes may not be useful in case of Cyber crime. Most of the time no fingerprints available, no blood stain, no DNA test analysis is useful to fix the identity of an individual. Moreover, he may not be essentially having presence within your national boundaries that causes difficulties in investigation of crime as well as arresting the criminals.

The nature of Cyber-crime is somewhat different from traditional crimes. Moreover, special category can be created under the banner of Cyber-criminality to provide different treatment to the crimes falling under this head. The plot of commission of crime may entirely different in case of Cyber-crime.

Therefore, for most of the traditional crime is concerned, physical presence of criminal is essential for commission of crime. Therefore while commission of traditional crime and afterwards we may trace out the presences of criminal on the scene. In such cases physical presence of an offender become most important question and his defense in the form of alibi play important role. However as Cyber-crime may be committed without being remain present on the actual scene of commission of crime, the techniques developed to trace out the offenders committing traditional offences are not more useful. In Cyber-crime, one may not find hairs, fingerprints, footprints, bloodstains, and smell of offenders. These sniffers (police dogs) are hardly having any use in case of Cyber-crime.

x. Cyber crime - the Space which does not recognize and respect territorial boundaries

The Cyberspace is the place where the entire place is opened for all surfers irrespective of his nationality. Everybody can enter into Cyber world without visa or passport. Thus Cyber Crime presents the nations of the world with a problem they have never before had to address, i.e., the permeability of national borders. Technology gives the ability to loot and inflict harm upon the entire world with little risk of apprehension and allows for experimenting with new varieties of criminal endeavors.[xxxii]

CYBER CRIME - MIXTURE OF TRADITIONAL AND MODERN

Some of the Cyber crime that appears in Cyber space is resemble with the traditional criminality only with the difference that they are committed in Cyberspace with the help of computers. Some of the Cyber crime that resemble with traditional crime fall in the categories of economic offences. Thus Cyber crime (that) ranges from economic offences (fraud, theft, industrial espionage, sabotage and extortion, product piracy, etc.) can be discussed on the same footing as if of traditional crime only with the difference that they have been committed with the help of computers. Therefore, while dealing with the crime similar with old-fashioned crime, only procedure will be different. However, some of the crimes committed in Cyber space are entirely new in varieties, e.g. infringements on privacy, propagation of illegal and harmful content, facilitation of prostitution and other moral offenses, and organized crime. At its most severe, Cyber crime borders on terrorism, encompassing attacks against human life and against national security establishments, critical infrastructure, and other vital veins of society. As these crimes involve a complex phenomenon either due to its special type or due to its transnational nature, it requires to be considered on entirely different footings.

CONCLUSION

Thus *may it be*, at conceptual and substantial level, Cyber crimes do not appear as a separate category and can be treated on the same footing with traditional crime; however, the analytical scrutiny reveals some different criterion for consideration. Some of the categories of Cyber crimes are definitely resemble with traditional crimes, but some are entirely new. At the same time the Trans-national nature of Cyber crime, compel the legal thinker to have second thought over it. Thus on the ground of Trans-nationality, global effect, technological involvement and non-applicability of traditional tools of investigation deserve separate jurisprudential approach for Cyber Crime.

At the same time, difference in various model of criminal justice system in different part of the world, different ideologies, principles, notions and objectives of each nation make Cyber crime more difficult to define and deal. Cross-border reflection of Cyber crime definitely requires separate procedure, investigative mechanism, and international cooperation and trans-national treatment. On this account, definitely, Cyber crime differs from traditional crime and capable of forming separate heads in penal laws and criminal procedure laws.

REFERENCES

[i] http://www.nytimes.com, David Post (Cyber law specialist, Temple Law School), 'Netiquette', visited on 8th Aug, 1999.

[ii] Reuters, 'Digital world still feeds no paper', *The Hindu Business Line, 8th Oct, 2000.*

[iii] See, Schedule V of the Information Technology (Certifying Authorities) Rules, 2000.

[iv] Jain Atul : Cyber Crime - Issues Threats and Management Vol. 1, Isha Books Delhi, pg. 3.

[v] *Charles Nesson & Anita Ramasastry, Cyber crime, http://Cyber.law.harvard.edu/studygroup/Cybercrime.html*

Last updated: June 22, 2002, accessed on 26 April 2005, 21:30:45

[vi] Jain Atul, *Cyber Crime : Issues Threats and Management*, (Vol I) Isha Books Delhi, pg. 4

[vii] Jain Atul : Cyber Crime - Issues Threats and Management Vol. 1, Isha Books Delhi, pg. 4

[viii] The example of dependence of human society on mechanical atomization can be evidenced by analyzing the impact of 9/11. The comparatively, suffering by human causality were less than impact on worldwide market economic.

[ix] http://pgd.iiita.ac.in/index_files/about.htm An article entitled, *'Cyber Law & Information Security'* on the web site of Indian Institute Of Information Technology - Allahabad

[x] http://www.indianchild.com/Cyber_crime_in_india.htm Accessed on 22.01.2005

[xi] http://pgd.iiita.ac.in/index_files/about.htm An article entitled, *'Cyber Law & Information Security'* on the web site of Indian Institute Of Information Technology - Allahabad

[xii] Diwan Parag, & Shammi Kapoor, *Cyber & E-Commerce Laws*, Bharat Publishing House, 2000.

[xiii] Vishwambharan, Anupama., 'The information super highway', The Indian Express, 12 May 1999.

[xiv] Menon Shailaja, *Protection of Intellectual Property in Cyber Space*, AuthorPress Delhi, Pg. 5.

[xv] Cyber laws : Intellectual property and e-commerce security - Edited by Krishna Kumar, Dominant Publishers and Distributors, New Delhi, pg. 295.

[xvi] For e.g. S. 40 of Indian Penal Code, 1860 only prescribe 'Offence' *denotes a thing made punishable by this code' but do not describe what is meant by Offence.*

[xvii] In 2008, an amendment has been made to add few more offences in the Information Technology Act, 2000

[xviii] http://www.cidap.gov.in/mainwccrime.aspx See also, same definition appeared on the web site of Cyber Crime Police Station, Banglore, Karnataka, http://www.Cyberpolicebangalore.nic.in/Cybercrimes.htm

[xix] Lunker Manish : *Cyber Laws: A Global Perspective pg. 2(An article from Internet) See* http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf. accessed on 22 September 2005. 21:52:15

[xx] http://www.rediff.com/netguide/index.html accessed on 23.01.2005

[xxi] See, Singh Balwinder, Addl, Sec, Central Vigilance Commission, Government of India, An article on Internet (in .pdf format) entitled, Cyber Crime - A new challenge for the police

[xxii] http://www.cidap.gov.in/documents/Cyber%20Crime%20-%20A%20new%20challenge%20for%20the%20Police_129200525502%20PM.pdf

[xxiii] http://www.legalserviceindia.com/articles/article.html - The Menace Of Cyber Crime by Anusuya Sadhu, Final year law student Symbiosis, Pune

[xxiv] see McConnell's : 'International Cyber-crimes & punishment – http://www.Cybercrimes.net Accessed on 26.12.2004

[xxv] http://www.niser.org.my/news/2004_11_22_01.html Accessed on 30.01.2005

[xxvi] http://www.niser.org.my/news/2004_11_22_01.html accessed 30.01.2005

[xxvii] *See, http://Cyber.law.harvard.edu/studygroup/Cybercrime.html Article entitled 'Cybercrime' by Charles Nesson, Anita Ramasastry.*

[xxviii] (21 of 2000)

[xxix] See Chapter XI 'Offenses' of Information Technology Act, 2000. Section 65 to 69.

[xxx] Though the Information Technology [Amendment] Act, 2008 has added few more categories of crime in the list, but this additions are still inadequate to accommodate the entire list of cyber crime under the one umbrella of the Information Technology Act, 2000

[xxxi] http://www.asianlaws.org/projects/network_crimes.htm accessed on 23.01.2005

[xxxii] Jain Atul, *Cyber Crime: Issues Threats and Management*, (Vol I) Isha Books Delhi, pg. 4

K@R@MS

http://www.karamsociety.org